Elementary Proof of the Remez Inequality

Borislav Bojanov

This note is concerned with the Tchebycheff polynomials $T_n(x)$. As well known they can be presented on $[-1,1]$ by the expression

$$T_n(x) = \cos(n \arccos x).$$

The famous Russian mathematician Pafnutii Lvovich Tchebycheff (1821–1894) introduced $T_n(x)$ as the polynomial of least uniform norm on $[-1,1]$ amid the polynomials of degree n with fixed leading coefficient.

The Tchebycheff polynomials appear prominently in various extremal problems posed in π_n (the set of all polynomials of degree n). An illuminating example is the classical Markov inequality, which shows that

$$\|p^{(k)}\| \leq \|T_n^{(k)}\|, \qquad k = 0, \dots, n,$$

for each $p \in \pi_n$ such that

$$\|p\| := \max\{|p(x)| : x \in [-1,1]\} \leq 1.$$

The proof of this and many other remarkable properties of T_n can be found in the recent book of Rivlin [4].

It has been mentioned already by Tchebycheff that T_n is the fastest growing polynomial outside $[-1,1]$. In other words,

$$\max\{|p(\xi)| : p \in \pi_n, \|p\| \leq 1\} = T_n(\xi)$$

for each $|\xi| \geq 1$. This observation provokes the following question: How large can a polynomial be given that it is constrained to be "small" on a substantial portion of its domain? Make the problem more precise as follows.

Let σ be an arbitrary fixed positive number. For every $p \in \pi_n$ define the set

$$M(p) := \{x \in [-1, 1+\sigma] : |p(x)| \leq 1\}.$$

Clearly $M(p)$ consists of mutually disjoint closed subintervals. Let $|M(p)|$ be the measure of $M(p)$, i.e., $|M(p)|$ is the total length of these subintervals. Denote

$$\pi_n(\sigma) := \{p \in \pi_n : |M(p)| \geq 2\}.$$

The problem is to characterize the polynomial p^* from $\pi_n(\sigma)$ which has a maximal uniform norm over $[-1, 1+\sigma]$.

Evidently, the Tchebycheff polynomial $T_n(x)$ belongs to $\pi_n(\sigma)$ for each $\sigma > 0$ since $|T_n(x)| \leq 1$ on $[-1,1]$ and $|T_n(x)| > 1$ for $|x| > 1$. In 1936 Remez [1]

established the following

$$\sup_{p\in\pi_n(\sigma)} \|p\|_\infty = \|T_n\|_\infty, \tag{1}$$

where the supremum norm is over $[-1, 1+\sigma]$. Of course $\|T_n\|_\infty = T_n(1+\sigma)$. The proof of (1) can be seen also in the book of Freud [2]. A simpler approach was found recently by Erdelyi [3]. We demonstrate here a short, elementary proof.

The proof: Note that for any fixed $x \in [-1, 1+\sigma]$ the quantity

$$\mu(x) := \sup\{|p(x)| : p \in \pi_n(\sigma)\}$$

is attained for some polynomial from $\pi_n(\sigma)$. We shall show first that $\mu(x) \le \mu(1+\sigma)$ for each $x \in [-1, 1+\sigma]$. Indeed, let x be an interior point of $[-1, 1+\sigma]$ and let p be the extremal polynomial for this point, i.e., $p \in \pi_n(\sigma)$ and $|p(x)| = \mu(x)$. Introduce the polynomials

$$p_1(x) := p(\alpha(x)), \qquad p_2(x) := p(\beta(x)),$$

where $\alpha\colon [-1, 1+\sigma] \to [-1, x]$ and $\beta\colon [-1, 1+\sigma] \to [x, 1+\sigma]$ are the linear transformations. Let M_1 and M_2 be the parts of $M(p)$ situated in $I_1 := [-1, x]$ and $I_2 := [x, 1+\sigma]$, respectively. Assuming that $|M_i| < \lambda |I_i|$ for $i = 1, 2$ and $\lambda = 2/(2+\sigma)$ we would get $|M| = |M_1 + M_2| < \lambda |I_1 + I_2| = \lambda(2+\sigma) = 2$, a contradiction. Therefore $|M_i|/|I_i| \ge \lambda$ at least for one i, say for $i = 1$. Then $|M(p_1)| \ge 2$ and hence $p_1 \in \pi_n(\sigma)$. This yields

$$\mu(x) = |p(x)| = |p_1(1+\sigma)| \le \mu(1+\sigma).$$

Therefore the Remez inequality will be proved if we show that

$$|p(1+\sigma)| \le T_n(1+\sigma) \quad \text{for each } p \in \pi_n(\sigma).$$

In order to show this, denote by $-1 = \eta_0 < \eta_1 < \cdots < \eta_n = 1$ the extremal points of T_n. We have

$$T_n(\eta_k) = (-1)^{n-k} \qquad k = 0, \dots, n. \tag{2}$$

Let $x_0 < x_1 < \cdots < x_n$ be the points of $M(p)$ which coincide with $\eta_0, \dots, \eta_n$ after we press $M(p)$ to the left, i.e., to the interval $[-1, M(p) - 1]$. By the Lagrange interpolation formula

$$|p(1+\sigma)| \le \sum_{k=0}^{n} \prod_{\substack{i=0\\ i\ne k}}^{n} \frac{|1+\sigma - x_i|}{|x_k - x_i|}$$

since $|p(x_i)| \le 1$. Now taking into account the obvious inequalities $|1+\sigma-x_i| \le |1+\sigma-\eta_i|$, $|x_k - x_i| \ge |\eta_k - \eta_i|$ and (2), we get

$$|p(1+\sigma)| \le \sum_{k=0}^{n} \prod_{\substack{i=0\\ i\ne k}}^{n} \frac{|1+\sigma-\eta_i|}{|\eta_k - \eta_i|} = T_n(1+\sigma).$$

The proof is completed.

The author is grateful to the referee and to the editor for their useful remarks.

REFERENCES

1. E. J. Remez, Sour une propriété de polynomes de Tchebysheff, *Communicationes le l'Inst. des Sci.*, Kharkov 13 (1936), 93–95.
2. G. Freud, *Orthogonal Polynomials*, Pergamon Press, Oxford, 1971.
3. T. Erdelyi, *Inequalities for generalized polynomials and their applications*, Ph.D. Thesis, University of South Carolina, 1989.
4. T. J. Rivlin, *Chebyshev Polynomials*, second edition, John Wiley & Sons, Inc., New York, 1990.

Department of Mathematics,
University of Sofia,
Boul. James Boucher 5,
1126 Sofia, BULGARIA

A Note on an Identity of Ramanujan

T. S. Nanjundiah

In a forthcoming paper [**1**], Berndt and Bhargava have supplied a proof of this eye-catching identity of Ramanujan found in his third notebook [**3**, p. 386]: if $ad = bc$, then

$$\begin{aligned}
&64\{(b+c+d)^6 - (a+c+d)^6 - (a+b+d)^6 + (a+b+c)^6 \\
&\qquad\qquad + (a-d)^6 - (b-c)^6\} \\
&\times\{(b+c+d)^{10} - (a+c+d)^{10} - (a+b+d)^{10} \\
&\qquad + (a+b+c)^{10} + (a-d)^{10} - (b-c)^{10}\} \\
&= 45\{(b+c+d)^8 - (a+c+d)^8 - (a+b+d)^8 \\
&\qquad + (a+b+c)^8 + (a-d)^8 - (b-c)^8\}^2.
\end{aligned}$$

It figures also in their expository article [**2**] featuring a selected group of Ramanujan's results. Unfortunately, they have missed its simple proof and so its genesis by not noticing that it is built from two sets of sums:

$$u_n = \alpha_1^n + \beta_1^n + \gamma_1^n, \quad \alpha_1 = b+c+d, \quad \beta_1 = -(a+b+c), \quad \gamma_1 = a-d,$$

$$v_n = \alpha_2^n - \beta_2^n + \gamma_2^n, \quad \alpha_2 = a+c+d, \quad \beta_2 = -(a+b+d), \quad \gamma_2 = b-c.$$

By $\alpha_j + \beta_j + \gamma_j = 0$, the underlying problem is to compute

$$\omega_n = \alpha^n + \beta^n + \gamma^n,$$

where α, β and γ are the roots of the cubic

$$z^3 - pz + q = 0.$$

It is simple to work out an easy special case of Newton's formulae for power sums of the roots of an algebraic equation. Indeed, the obvious recursion

$$\omega_{n+3} - p\omega_{n+1} + q\omega_n = 0$$

with the initial values

$$\omega_{-1} = \frac{p}{q}, \qquad \omega_0 = 3, \qquad \omega_1 = 0,$$

yields

$$\omega_2 = 2p, \qquad \omega_4 = 2p^2,$$

$$\omega_3 = -3q, \qquad \omega_5 = 5pq, \qquad \omega_7 = -7p^2q,$$

$$\omega_6 = 2p^3 + 3q^2, \qquad \omega_8 = 2p^4 + 8pq^2, \qquad \omega_{10} = 2p^5 + 15p^2q^2.$$

Form the cubic whose roots are α_j, β_j and γ_j:

$$z^3 - p_j z + q_j = 0.$$

We have

$$p_1 = (b + c + d)(a + b + c) + (a - d)^2,$$

$$p_2 = (a + c + d)(a + b + d) + (b - c)^2,$$

$$p_1 - p_2 = 3(bc - ad).$$

Hence $p_1 = p_2$ if and only if

$$ad = bc.$$

Assume this condition and set

$$p_1 = p_2 = P, \qquad \Delta = q_1^2 - q_2^2.$$

Now the $u_n = \omega_n(p_1, q_1)$ and the $v_n = \omega_n(p_2, q_2)$ given by the computed $\omega_n = \omega_n(p, q)$ show that

$$u_2 = v_2, \qquad u_4 = v_4,$$

$$u_6 - v_6 = -3\Delta, \qquad u_8 - v_8 = 8P\Delta, \qquad u_{10} - v_{10} = 15P^2\Delta.$$

So we have Ramanujan's ingenious parametric construction of equal sums of three nth powers ($n = 2, 4$), and Ramanujan's identity. Clearly, for both these results, the condition $ad = bc$ is crucial. Ramanujan must have been primarily looking for the first one because of its number-theoretic signifiance, the second being incidental and apparently the only one of its kind in this context.

For special choices of the parameters, the equal sums of three nth powers ($n = 2, 4$) constructed by Ramanujan may present the same terms! This happens, for instance, when

$$a = b\ (c = d), \qquad a = c\ (b = d), \qquad b = 0 = d\ (a \neq 0), \qquad c = 0 = d\ (a \neq 0).$$

Barring such cases, the construction yields numbers expressible as sums of three nth powers ($n = 2, 4$) in two different ways. This observation, which we owe to a comment of the referee/editor, does not point to any flaw in the construction for which what really matters is its *algebraic* formulation.

I wish to thank Professor Bhargava for having kindly shown me the proof sheets of [1] and a preprint of [2].

REFERENCES

1. Bruce C. Berndt and S. Bhargava, A remarkable identity found in Ramanujan's third notebook, *Glasgow Math. J.* 34 (1992) 341–345.
2. Bruce C. Berndt and S. Bhargava, Ramanujan—for Lowbrows, this MONTHLY (to appear).
3. S. Ramanujan, *Notebooks* (2 vols.), Tata Institute of Fundamental Research, Bombay, 1957.

180, I Cross
Gangotri Layout–I Stage
Mysore-570 009
India

On an Identity of Daubechies

Doron Zeilberger

Tossing a coin (whose $Pr(head) = p$) until reaching n heads or n tails and equating the probability, 1, of finishing with the sum of the probabilities of all the possible final outcomes leads to

$$\sum_{i=0}^{n-1} \binom{n+i-1}{i} p^n (1-p)^i + \sum_{i=0}^{n-1} \binom{n+i-1}{i} p^i (1-p)^n = 1,$$

which was proved in [1], (pp. 167–171) and [2] using Bezout's theorem and induction respectively. Rolling a k-faced die instead leads to the multivariate generalization

$$\sum_{i=1}^{k} \sum_{\substack{0 \le \alpha_j \le n-1 \\ j \ne i}} \frac{(\alpha_1 + \cdots + \alpha_{i-1} + (n-1) + \alpha_{i+1} + \cdots + \alpha_k)!}{\alpha_1! \ldots \alpha_{i-1}!(n-1)!\alpha_{i+1}! \ldots \alpha_k!} \times$$

$$p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_i^n p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k} = 1,$$

provided $p_1 + \cdots + p_k = 1$.

REFERENCES

1. Ingrid Daubechies, Ten lectures on wavelets, *SIAM*, Philadelphia, 1992.
2. ______, Orthogonal bases of compactly supported wavelets, *Comm. Pure Appl. Math.*, 41 (1988), 909–996.

Department of Mathematics
Temple University
Philadelphia, PA 19122
zeilberg@euclid.math.temple.edu

COMPUTER SCIENCE SAMPLER

Edited by: **Catherine C. McGeoch**

In the May 1968 issue of the Monthly, G. E. Forsythe wrote an article titled "What to do till the computer scientist comes." Among his several suggestions: "Read [about computer science]. Since computer science is not yet very deep and mathematicians are very smart people, this should not be onerous."

There is no doubt that the ties between mathematics and computer science are strong and that each field has had a profound influence upon the other. It is also true that computer science (and mathematics) has changed and developed considerably since the 1960's. In the "Computer Science Sampler" I and guest columnists will try and give a glimpse of what computer scientists have been up to lately: we will write about intriguing mathematical results, old and new, that make possible the development of modern computing machines and computational methods.

Although computer science has gotten a lot "deeper" in the 20 years since Forsythe's article, reading the columns should not be onerous. After all, mathematicians are still very smart people.

Data Compression

Catherine C. McGeoch

Every object stored in a computer, whether an integer, the text of the *Oxford English Dictionary*, or a digitized image of the Mona Lisa, must first be *encoded* into a sequence of 0's and 1's (called bits). Alphabetic characters are usually represented according to either the ASCII (ask-ee) or the EBCDIC (ib-se-dic) standard code. For example, "A" is encoded 01000001 in ASCII and 11000001 in EBCDIC.

Suppose you want to store the text of *Far from the Madding Crowd* by Thomas Hardy. The book contains 768,771 characters: since both standard codes use 8 bits (one byte) per character the book would occupy slightly over half of a 3.5 inch floppy disk. Methods of *data compression* can be applied so that Hardy's book requires an average of 2.48 bits per character [**1**], thereby reducing the storage requirements by a factor of three.

Samuel Morse used a form of data compression in the design of his famous code. The frequently used letters have short sequences (E and T are · and –·), and the less common letters have long sequences (Y and Z are –·–– and ––··). Although an alphabet of 30 characters requires $3.26 = [2 \cdot 1 + 4 \cdot 2 + 8 \cdot 3 + 14 \cdot 4]/30$ bits per character on average (using two 1-bit codes, four 2-bit codes, and so on), we might expect that a message in Morse Code would be shorter than

average because letters with short codes appear frequently. In this column we shall examine a data compression scheme that produces optimally-short encodings.

First, some definitions. An *alphabet* is a finite set of characters. We will denote a special alphabet $\beta = \{0, 1\}$. A *word* is a finite sequence of characters from some alphabet. (Although examples in this column will use "natural English" words, this need not be the case in general.) A *message* is a sequence of words. A *code* C is a one-to-one onto function mapping a set of *source words* $W = \{w_1, w_2,, \ldots, w_n\}$ from some alphabet to a set of *code words* $\{b_1, \ldots b_n\}$ from β. We *encode* a sequence of source words by applying C to each word in sequence. We *decode* a message by applying the inverse function C' to the coded words.

A *prefix code* is one in which no code word is a proper prefix of another. Prefix codes are desirable because it is easy to break a coded message into words when decoding. Figure 1, for example, shows two codes for a word set W. Code C_1 is a prefix code and C_2 is not. There is no ambiguity decoding $M = 1111100110$ according to C_1, but decoding with C_2 produces (at least) two different source messages.

P	W	C_1	C_2
.40	not	110	11
.35	save	00	11111
.14	the	01	001
.06	trust	111	111
.05	queen	10	10

Figure 1. Two codes for the same set of source words. The first is a prefix code, the second is not.

Let us assume that the source words $W = \{w_1, \ldots, w_n\}$ appear in source messages according to some fixed probability distribution $P = \{p_1, \ldots, p_n\}$. For a particular code C, let $l(C, i)$ denote the length (number of bits) in $C(w_i)$. The expected word length in a random coded message is therefore $L(C) = \Sigma_{i=1}^{n} p_i \cdot l(C, i)$. Given W and P, how shall we construct an *optimal* prefix code having minimum expected word length?

Good question. Is C_1 an optimal prefix code for the probabilities given in Figure 1? Can you find a better code?

HUFFMAN CODES. In 1952 D. A. Huffman developed an elegant and efficient method for constructing optimal prefix codes given W and P. He did this by building an *encoding tree*, which is a binary tree such that every node j has an associated *cost* c_j and has either 2 or 0 children. Each source word w_i is represented by a *leaf* node i in the tree having cost assigned such that $c_i = p_i$. Left branches in encoding trees are labeled 0 and right branches are labeled 1.

Every prefix code C is represented by an encoding tree T_C. In Figure 2, for example, the encoding $C_1(queen) = 10$ is found by reading edge labels downward from the root to the leaf labeled "queen". The prefix property is ensured because no word is an ancestor of another in the tree.

The *depth* d_i of node i is its distance from the root. The *weighted path length* of leaf node i is $a_i = p_i \cdot d_i$. The *average path length* $PL(T_C)$ of the tree is found by summing weighted path lengths over leaves and is therefore equal to the expected word length $L(C)$ of the code. In Figure 2, the "queen" node has depth 2 and weighted path length .10. The average path length for this tree is 2.46.

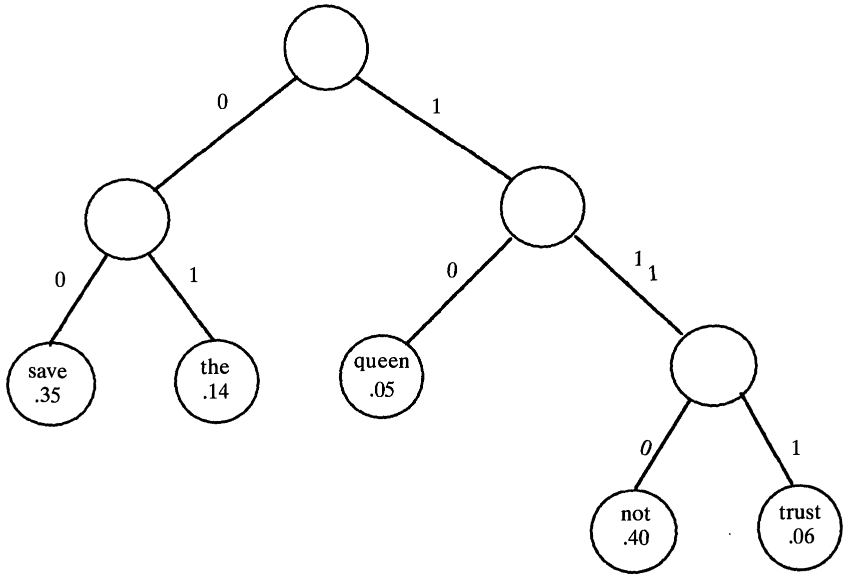


Figure 2. An encoding tree for code C_1.

Huffman's tree construction method works as follows.

1. Begin with a list of one-node trees corresponding to words $w_1 \dots w_n$ and having costs $c_1 \dots c_n$ equal to $p_1 \dots p_n$ respectively.
2. Repeat the next two steps $n - 1$ times:
3. Find two trees Q and R in the list having smallest costs c_q and c_r at their root nodes (breaking ties arbitrarily). Remove them from the list.
4. Construct a new tree S as follows. Make a new root node s having Q as its left subtree and R as its right subtree. The cost of node s is $c_s = c_q + c_r$. Add tree S to the list.

At the end of this process the list will contain a single encoding tree, called a *Huffman tree*. We shall prove that any Huffman tree has minimal average path length.

Theorem. *Let T_h be a Huffman tree constructed for a given set of words W and probabilities P. Then for any encoding tree T constructed on W and P, $PL(T_h) \leq PL(T)$.*

Proof: The proof is by induction on the number of leaves in T_h. If T_h has one or two leaves the encoding tree is unique and the proof is trivial.

Suppose T_h has $n > 2$ leaves and let nodes i and j be the nodes of minimal cost that were selected in the first step of the construction. These are necessarily leaf nodes in T_h and they are necessarily siblings (having a common parent node). Construct a new tree T_h' containing $n - 1$ leaves by removing i and j: their common parent node x becomes a new leaf having cost $c_x = c_i + c_j$. Since the

only effect of this modification is to move the combined cost c_x one level closer to the root, we have $PL(T_h) = PL(T_h') + c_x$.

Let w_x be formed by the concatenation of w_i and w_j and let $p_x = p_i + p_j$. Then T_h' is a Huffman tree constructed on the word set $W' = W - \{w_i, w_j\} + \{w_x\}$ with probabilities $P' = P - \{p_i, p_j\} + \{p_x\}$.

Now construct a tree T' from T by removing the same nodes i and j and replacing them with a new node y. Since T is an encoding tree for W these are necessarily leaf nodes, but they are not necessarily siblings in T. We have two cases:

1. If i and j are siblings then remove them and form a new leaf node from the parent x exactly as was done for T_h. The new tree T' is an encoding tree for W' and P', and $PL(T) = PL(T') + c_x$,
2. If i and j are not siblings then adjust the tree to make them siblings: if i has greater depth than j exchange j with the sibling of i, and if j has greater depth than i exchange i with the sibling of j (if they have equal depth then it doesn't matter which gets exchanged). That is, suppose $d_i > d_j$ and that node s is the sibling of i. Detach the subtree having root s and move it (up) to j's place in the tree, and move j (down) to s's location in the tree. (The case $d_i < d_j$ is handled similarly.)

   Moving j increases its depth by $\delta = d_i - d_j$ and increases the average path length of the tree by δc_j. But every leaf node that is moved along with s has its path length *decreased* by δ: since j was chosen to have minimal cost (except possibly for i), the net effect of the exchange operation cannot be an increase in average path length. Letting T_0 denote the new tree, we have $PL(T_0) \le PL(T)$.

   Now Case 1 holds. Remove nodes i and j and replace with x as above to form T' from T_0. Then $PL(T') + c_x = PL(T_0) \le PL(T)$.

By the induction hypothesis $PL(T_h') \le PL(T')$. Combining this with the above inequalities completes the proof. □

OTHER CODES. One practical problem with Huffman's Code is that either the probabilities P must be estimated beforehand or the text to be encoded must be pre-scanned to determine word frequencies. This leads to inefficiencies in either the length of coded messages or in the time required to encode messages. A *dynamic* code C allows the mapping of source words to code words to change "on the fly" as the message is being encoded. Some methods (most notably Lempel-Ziv encodings) modify W dynamically as well as C. The compression factor of three mentioned earlier for Hardy's text is achieved by a dynamic method that combines several compression ideas [**1**].

Some codes are specialized for data other than (English) text. A digitized image of the Mona Lisa, for example, will tend to have long sequences of identical source words (which represent colors and intensities). *Run-length encoding* maps a sequence such as *yyyyyyyyybbbbbbggrrrrrrrrrr* into a sequence of pairs $9y, 6b, 2g, 10r$ which may be compressed further.

For a detailed discussion of static and dynamic Huffman codes and of the Lempel-Ziv method, see Lewis and Denenberg [**2**]. Lelewer and Hirshberg [**3**] provide an extensive and detailed survey of several data compression schemes along with some experimental comparisons. Several methods for data modeling with applications to text compression are surveyed by Bell et al. [**1**].

REFERENCES

1. T. Bell, I. H. Witten, and J. G. Cleary, Modeling for text compression, *ACM Computing Surveys*, (21)4, December 1989, pp. 557–591.
2. H. R. Lewis and L. Denenberg, *Data Structures and Their Algorithms*, Harper-Collins 1991.
3. D. A. Lelewer and D. S. Hirschberg, Data compression, *ACM Computing Surveys*, (19)3, September 1987, pp. 261–296.

Department of Mathematics and Computer Science
P.O. Box 2239
Amherst College
Amherst, MA 01002
ccm@cs.amherst.edu

It is the consensus of opinion among college teachers of mathematics (See J. Seidlin, Mathematics Teacher, Dec. 1932) and science that the secondary schools produce graduates with the following general characteristics:

(1) Worn out or weary of mathematics,
(2) No inspiration for individual investigation,
(3) No appreciation of accuracy,
(4) Not able to place a decimal point in its proper place,
(5) Direct and inverse proportions are meaningless.

—*American Mathematical Monthly*
40, (1933) p. 382

PROBLEMS AND SOLUTIONS

Edited by:
Richard T. Bumby, Fred Kochman and Douglas B. West

Proposed problems should be sent to the MONTHLY PROBLEMS address given on the inside front cover. Please include solutions, relevant references, etc. Three copies are requested.

Solutions of published problems should arrive before October 31, 1993 at the MONTHLY PROBLEMS address given on the inside front cover. Solutions should be typed with double spacing, including the problem number and the solver's name and mailing address. Two copies suffice. A self-addressed postcard or label should be included if an acknowledgment is desired.

*An asterisk (*) after the number of a problem, or part of a problem, indicates that no solution is currently available. Partial solutions will be useful in such cases. Otherwise, the published solution is likely to be based on a solution which is complete and correct. Of course, an elegant partial solution or a method leading to a more general result is always useful and welcome. In addition, references to other appearances of MONTHLY problems or to solutions of these problems in the literature are also solicited.*

PROBLEMS

10306. *Proposed by Seung-Jin Bang, Seoul, Korea.*

Find all positive integers n such that the polynomial

$$a^n(b-c)+b^n(c-a)+c^n(a-b)$$

has $a^2+b^2+c^2+ab+bc+ca$ as a factor.

10307. *Proposed by John Calvin Williams, student, and I. Martin Isaacs, University of Wisconsin, Madison, WI.*

Can one construct a set $\mathscr{X}$ of finite groups satisfying the two conditions:

i. $\mathscr{X}$ contains precisely one representative from each isomorphism class.

ii. If $A \in \mathscr{X}$ is isomorphic to a subgroup of $B \in \mathscr{X}$, then A *is* a subgroup of B.

10308. *Proposed by Robert Connelly and John H. Hubbard, Cornell University, Ithaca, NY, and Walter Whiteley, York University, North York, Ontario, Canada.*

Suppose that $p_1, p_2, p_3, q_1, q_2, q_3$ are six points in the plane and that the distance between p_i and q_j $(i, j = 1, 2, 3)$ is $i + j$. Show that the six points are collinear.

10309. *Proposed by Walter Rudin, University of Wisconsin, Madison, WI.*

Compute

$$\exp\left(\frac{1}{2\pi}\int_{-\pi}^{\pi}\log(A + B\cos\theta)\, d\theta\right)$$

when $A > B > 0$. The answer should be given as an algebraic function of A and B.

10310. *Proposed by E. Rodney Canfield, University of Georgia, Athens, GA.*

Fix an integer $r \geq 2$. Using Stirling's formula we may find constants c_1 and c_2 such that

$$\binom{rm}{m} \sim \frac{c_1(c_2)^m}{m^{1/2}}$$

as $m \to \infty$. Prove that the ratio $\binom{rm}{m} m^{1/2}/c_2^m$ is an increasing function of m for $m \geq 1$.

10311. *Proposed by Solomon W. Golomb, University of Southern California, Los Angeles, CA.*

It is well-known that if g is a primitive root modulo p, where $p > 2$ is prime, either g or $g + p$ (or both) is a primitive root modulo p^2 (indeed modulo p^k for all $k \geq 1$).

(a) Find an example of a prime $p > 2$, and a primitive root g modulo p with $1 < g < p$ such that g is *not* a primitive root modulo p^2.

(b) Show that, among all $\phi(p-1)$ primitive roots g modulo p with $1 < g < p$, at least half of them are also primitive roots modulo p^2.

10312. *Proposed by Hongyuan Zha, IMA—University of Minnesota, Minneapolis, MN.*

Let c and s be non-negative real numbers satisfying $c^2 + s^2 = 1$. Prove that, for $n > 1$,

$$s^{n-2}\sqrt{1+c}$$

is the *second* smallest singular value of the n by n upper triangular matrix

$$T_n(c) = \operatorname{diag}(1, s, \cdots, s^{n-1})\begin{pmatrix} 1 & -c & -c & \cdots & -c \\ & 1 & -c & \cdots & -c \\ & & \ddots & \ddots & \vdots \\ & & & 1 & -c \\ & & & & 1 \end{pmatrix}.$$

10313. *Proposed by O. Krafft and M. Schaefer, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany.*

Let $a \in [-1/5, 1)$ and let $\mathscr{X}_a$ denote the set of random variables X satisfying $a \leq X \leq 1$. Show that

$$\max\left\{EX^2EX^4 - (EX^3)^2 \colon X \in \mathscr{X}_a\right\} = 2^{-6}$$

if and only if $a \in [-1/5, 1/2]$.

NOTES

Notes: (10311) The multiplicative group modulo the power of an odd prime is always cyclic, and the term *primitive root* is the traditional name in elementary number theory for a generator of this group. Fundamental properties can be found in textbooks such as I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers* (fifth edition). A consequence of (b) is that for every prime $p > 2$ there is at least one g with $1 < g < p$ which is a primitive root modulo p^k for all $k \geq 1$. **(10312)** The matrix $T_n(c)$ is a well known example in numerical linear algebra. More details can be found in G. Golub & C. Van Loan, *Matrix Computations*. It should be noted that there is no simple expression for the smallest singular value of $T_n(c)$.

SOLUTIONS

Solving the Velocity Composition Equation of Special Relativity

6659 [1991, 445]. *Proposed by Abraham Ungar, North Dakota State University, Fargo, ND.*

Let $\mathbb{R}_c^3$ be the subset of the Euclidean 3-space $\mathbb{R}^3$ given by the equation

$$\mathbb{R}_c^3 = \{\mathbf{x} \in \mathbb{R}^3 \colon |\mathbf{x}| < c\},$$

where c is a positive constant. In the special theory of relativity c represents the speed of light, and the elements $\mathbf{x}$ of $\mathbb{R}_c^3$ are *admissible velocities*. The relativistic velocity composition law is given by the equation

$$\mathbf{x} * \mathbf{y} = \frac{\mathbf{x} + \mathbf{y}}{1 + \mathbf{x} \cdot \mathbf{y}/c^2} + \frac{1}{c^2} \cdot \frac{\gamma_{\mathbf{x}}}{\gamma_{\mathbf{x}} + 1} \cdot \frac{\mathbf{x} \times (\mathbf{x} \times \mathbf{y})}{1 + \mathbf{x} \cdot \mathbf{y}/c^2}, \qquad \mathbf{x}, \mathbf{y} \in \mathbb{R}_c^3,$$

where $\gamma_{\mathbf{x}}$ is the *Lorentz factor*

$$\gamma_{\mathbf{x}} = \frac{1}{\sqrt{1 - \mathbf{x} \cdot \mathbf{x}/c^2}}.$$

It is known that the space $\mathbb{R}_c^3$ is closed under the relativistic velocity composition: if $\mathbf{x}, \mathbf{y} \in \mathbb{R}_c^3$ then $\mathbf{x} * \mathbf{y} \in \mathbb{R}_c^3$.

For given $\mathbf{a}, \mathbf{b} \in \mathbb{R}_c^3$ solve each of the two velocity composition equations

$$\mathbf{a} * \mathbf{x} = \mathbf{b} \tag{1}$$

and

$$\mathbf{x} * \mathbf{a} = \mathbf{b} \tag{2}$$

for the unknown $\mathbf{x} \in \mathbb{R}_c^3$.

Solution by Rolf Richberg, RWTH Aachen, Aachen, Germany. For $\mathbf{x} \in \mathbb{R}_c^3$, $\mathbf{x}/c \in \mathbb{R}_1^3$ and this rescaling is compatible with the definitions of $*$ in $\mathbb{R}_c^3$ and $\mathbb{R}_1^3$, so it suffices to consider $\mathbb{R}_1^3$. In this case $\gamma_{\mathbf{x}} = (1 - \mathbf{x} \cdot \mathbf{x})^{-1/2}$. Elementary vector algebra then yields that

$$\mathbf{x}*\mathbf{y} = \frac{\gamma_{\mathbf{x}}}{1+\gamma_{\mathbf{x}}}\left(1 + \frac{1}{\gamma_{\mathbf{x}}(1+\mathbf{x}\cdot\mathbf{y})}\right)\mathbf{x} + \frac{1}{\gamma_{\mathbf{x}}(1+\mathbf{x}\cdot\mathbf{y})}\mathbf{y} \tag{A}$$

$$\mathbf{x}\cdot(\mathbf{x}*\mathbf{y}) = 1 - \frac{1}{\gamma_{\mathbf{x}}^2(1+\mathbf{x}\cdot\mathbf{y})} \tag{B}$$

$$\gamma_{\mathbf{x}*\mathbf{y}} = \gamma_{\mathbf{x}}\gamma_{\mathbf{y}}(1+\mathbf{x}\cdot\mathbf{y}) \tag{C}$$

$$(-\mathbf{x})*(\mathbf{x}*\mathbf{y}) = \mathbf{y} \tag{D}$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}_1^3$. The special case

$$\mathbf{x}*\mathbf{x} = \frac{2}{1+\mathbf{x}\cdot\mathbf{x}}\mathbf{x}$$

of (A) is also worthy of note. It is now a simple matter to solve equation (1). From (D), we know that $\mathbf{a}*((-\mathbf{a})*\mathbf{b}) = \mathbf{b}$, which shows that $\mathbf{x} = (-\mathbf{a})*\mathbf{b}$ is a solution to (1). On the other hand, (1) implies that $(-\mathbf{a})*\mathbf{b} = (-\mathbf{a})*(\mathbf{a}*\mathbf{x}) = \mathbf{x}$. Thus (1) has the sole solution $\mathbf{x} = (-\mathbf{a})*\mathbf{b}$.

A slightly greater effort is required to solve equation (2). Assuming that $\mathbf{x}$ is a solution of (2), (C) yields $\gamma_{\mathbf{x}}(1 + \mathbf{x}\cdot\mathbf{a}) = \gamma_{\mathbf{b}}/\gamma_{\mathbf{a}}$. Then (A) gives

$$\begin{aligned}\gamma_{\mathbf{b}}\mathbf{b} &= \frac{\gamma_{\mathbf{b}}\gamma_{\mathbf{x}}}{1+\gamma_{\mathbf{x}}}\left(1 + \frac{1}{\gamma_{\mathbf{x}}(1+\mathbf{a}\cdot\mathbf{x})}\right)\mathbf{x} + \frac{\gamma_{\mathbf{b}}}{\gamma_{\mathbf{x}}(1+\mathbf{a}\cdot\mathbf{x})}\mathbf{a} \\ &= \frac{\gamma_{\mathbf{x}}}{1+\gamma_{\mathbf{x}}}(\gamma_{\mathbf{b}} + \gamma_{\mathbf{a}})\mathbf{x} + \gamma_{\mathbf{a}}\mathbf{a}.\end{aligned}$$

Now, let

$$\mathbf{v} = \frac{\gamma_{\mathbf{x}}}{1+\gamma_{\mathbf{x}}}\mathbf{x} = \frac{\gamma_{\mathbf{b}}\mathbf{b} - \gamma_{\mathbf{a}}\mathbf{a}}{\gamma_{\mathbf{b}} + \gamma_{\mathbf{a}}}.$$

In view of $\mathbf{v}\cdot\mathbf{v} = (\gamma_{\mathbf{x}} - 1)/(\gamma_{\mathbf{x}} + 1)$, we have $\gamma_{\mathbf{x}} = (1 + \mathbf{v}\cdot\mathbf{v})/(1 - \mathbf{v}\cdot\mathbf{v})$ and

$$\mathbf{x} = \frac{2}{1+\mathbf{v}\cdot\mathbf{v}}\mathbf{v} = \mathbf{v}*\mathbf{v}.$$

On the other hand, given $\mathbf{a}, \mathbf{b} \in \mathbb{R}_1^3$, define $\mathbf{v} = (\gamma_{\mathbf{b}}\mathbf{b} - \gamma_{\mathbf{a}}\mathbf{a})/(\gamma_{\mathbf{b}} + \gamma_{\mathbf{a}})$ and $\mathbf{x} = \mathbf{v}*\mathbf{v}$. Then, using (C), we get

$$\mathbf{v}\cdot\mathbf{v} = 1 - 2\frac{1+\gamma_{\mathbf{a}*\mathbf{b}}}{(\gamma_{\mathbf{b}} + \gamma_{\mathbf{a}})^2} < 1.$$

Also

$$\mathbf{x}\cdot\mathbf{x} = 1 - \left(\frac{1-\mathbf{v}\cdot\mathbf{v}}{1+\mathbf{v}\cdot\mathbf{v}}\right)^2 < 1$$

yields

$$\gamma_{\mathbf{x}} = \frac{1+\mathbf{v}\cdot\mathbf{v}}{1-\mathbf{v}\cdot\mathbf{v}} \quad \text{and} \quad \mathbf{v} = \frac{\gamma_{\mathbf{x}}}{1+\gamma_{\mathbf{x}}}\mathbf{x}.$$

Now, by (C)

$$2\mathbf{a}\cdot\mathbf{v} = \frac{2}{\gamma_{\mathbf{b}}+\gamma_{\mathbf{a}}}\left(\gamma_{\mathbf{b}}\left(\frac{\gamma_{\mathbf{a}*\mathbf{b}}}{\gamma_{\mathbf{a}}\gamma_{\mathbf{b}}}-1\right)-\gamma_{\mathbf{a}}\left(1-\frac{1}{\gamma_{\mathbf{a}}^2}\right)\right)$$
$$= \frac{2(1+\gamma_{\mathbf{a}*\mathbf{b}})}{\gamma_{\mathbf{a}}(\gamma_{\mathbf{b}}+\gamma_{\mathbf{a}})}-2$$
$$= \frac{\gamma_{\mathbf{b}}}{\gamma_{\mathbf{a}}}(1-\mathbf{v}\cdot\mathbf{v})-1-\mathbf{v}\cdot\mathbf{v},$$

and hence

$$\gamma_{\mathbf{x}}(1+\mathbf{a}\cdot\mathbf{x}) = \frac{1+\mathbf{v}\cdot\mathbf{v}}{1-\mathbf{v}\cdot\mathbf{v}}\left(1+\frac{2}{1+\mathbf{v}\cdot\mathbf{v}}\mathbf{a}\cdot\mathbf{v}\right) = \frac{\gamma_{\mathbf{b}}}{\gamma_{\mathbf{a}}},$$

which, with (A) yields

$$\mathbf{x}*\mathbf{a} = \left(1+\frac{\gamma_{\mathbf{a}}}{\gamma_{\mathbf{b}}}\right)\mathbf{v}+\frac{\gamma_{\mathbf{a}}}{\gamma_{\mathbf{b}}}\mathbf{a} = \mathbf{b}.$$

This settles the case of equation (2). These formulas: $\mathbf{x} = (-\mathbf{a})*\mathbf{b}$ in (1); and $\mathbf{x} = \mathbf{v}*\mathbf{v}$ with $\mathbf{v} = (\gamma_{\mathbf{b}}\mathbf{b}-\gamma_{\mathbf{a}}\mathbf{a})/(\gamma_{\mathbf{b}}+\gamma_{\mathbf{a}})$ in (2) use only expressions preserved by the mappings used to rescale c. Hence they are valid for all $c > 0$.

Editorial comment. The proposer's proof is contained in his paper, "Thomas precession and its associated grouplike structure", *Am. J. Phys.* 59 (1991), 824–834, which explores the abstract algebraic properties of addition of velocities in special relativity. In particular, weak versions of associative and commutative laws can be found which enable equations (1) and (2) to be solved by operations resembling those used in associative algebras.

Thomas N. Delmer approached the problem by analogy to the use of quaternions to study rotations in Euclidean 3-space. The matrix

$$T(\mathbf{x}) = \begin{pmatrix} \gamma_x & -\gamma_{\mathbf{x}}\mathbf{x}^T/c \\ -\gamma_{\mathbf{x}}\mathbf{x}/c & I+(\gamma_{\mathbf{x}}-1)\mathbf{x}\mathbf{x}^T/|\mathbf{x}|^2 \end{pmatrix}$$

describes the left action of $\mathbf{x}$ on columns occurring as first columns of $T(\mathbf{y})$ for $\mathbf{y}\in\mathbb{R}_c^3$. The solution of equation (1) follows from the fact that $T(\mathbf{x})^{-1} = T(-\mathbf{x})$. To solve equation (2), one *linearizes* the problem by writing $T = CC^T$ where C is a matrix whose inverse is its complex conjugate $\overline{C}$ and whose entries depend linearly on four real parameters. The equation $T\mathbf{a} = \mathbf{b}$ then takes the form $C^T\mathbf{a} = \overline{C}\mathbf{b}$, which is a system of linear equations in the parameters defining C. This use of the matrix C corresponds to the vector $\mathbf{v}$ in the solution above.

Solved also by R. J. Chapman (U.K.), T. N. Delmer, S. Eder (student, Austria), M. Golomb, T. L. McCoy, K. McInturff, and the proposer. Two incorrect solutions were received.

An Aperiodic Sequence

E 3457 [1991, 754]. *Proposed by Herbert S. Wilf, University of Pennsylvania, Philadelphia, PA.*

Find all positive integers k such that the sequence

$$\left\{\binom{2n}{n}\right\}_{n=0}^{\infty}$$

is periodic modulo k from some point onward.

Solution by Jerrold R. Griggs, University of South Carolina, Columbia, SC. The only such values of k are 1 and 2. The case $k = 1$ is trivial, while for $k = 2$ the familiar binomial coefficient recursion and symmetry yields

$$\binom{2n}{n} = \binom{2n-1}{n} + \binom{2n-1}{n-1} = 2\binom{2n-1}{n-1} \equiv 0 \pmod 2$$

for all $n \geq 1$.

Next let $k = 4$. By the binomial theorem, $\binom{2n}{n} \pmod 4$ is the coefficient of x^n in the expansion of $(1+x)^{2n}$ over $Z_4[x]$. We claim that $(1+x)^{2^m} = 1 + 2x^{2^{m-1}} + x^{2^m}$ over $Z_4[x]$ for $m \geq 1$. This is immediate for $m = 1$ and readily verified for $m > 1$ by induction on m by multiplying out $(1+x)^{2^{m+1}} = ((1+x)^{2^m})^2$. Hence $\binom{2n}{n} \equiv 2 \pmod 4$ when $n = 2^j$ for $j \geq 0$. On the other hand, if $n \geq 3$ is not a power of 2, say $n = 2^j + r$ where $0 < r < 2^j$, we obtain over $Z_4[x]$ that

$$(1+x)^{2n} = (1+x)^{2^{j+1}}(1+x)^{2r} = (1 + 2x^{2^j} + x^{2^{j+1}})(1+x)^{2r}.$$

Since $2r < n < 2^{j+1}$, the only contribution to the coefficient of x^n is $2\binom{2r}{r}$, which is divisible by 4 since $\binom{2r}{r}$ is divisible by 2. Hence $\left\{\binom{2n}{n}\right\}$ is not eventually periodic mod 4, as it contains arbitrarily long finite stretches of zeroes modulo 4.

Next suppose that k is an odd prime p. Since $p \mid \binom{p}{i}$ for all $0 < i < p$, we have $(1+x)^p = 1 + x^p$ over $Z_p[x]$. By induction, it follows for $m \geq 1$ that $(1+x)^{p^m} = 1 + x^{p^m}$. Hence for $0 \leq j < p^m$ the coefficient of x^i in $(1+x)^{p^m+j}$ is 1 for $i = j$ and $i = p^m$ but 0 for $j < i < p^m$. Also, the coefficient of x^{p^m} in $(1+x)^{2p^m}$ is 1 mod p. Again, the sequence $\left\{\binom{2n}{n} \bmod k\right\}$ contains arbitrarily long finite stretches of zeroes and cannot be eventually periodic.

Each remaining value of k is divisible by an odd prime or by 4; call this divisor d. The sequence cannot by eventually periodic mod k, else it would be eventually periodic mod d as well, which we have shown cannot happen.

Solved also by R. J. Chapman (U.K.), P. Čížek (student, France), M. Dindos (Slovakia), R. B. Eggleton (Brunei), N. J. Fine, I. Gessel, R. Holsager, I. Kastanas, K. S. Kedlaya (student), N. Komanda, O. P. Lossers (The Netherlands), D. Magagnosc, I. Nemes (Austria), A. Nijenhuis, A. Pedersen (Denmark), B. Peterson, N. G. Randolph, I. Vardi, Con Amore Problem Group (Denmark), and the proposer.

Subsets Whose Sums Are Congruent

E 3472 [1991, 956]. *Proposed by Hunter Snevily, California Institute of Technology, Pasadena, CA.*

Suppose h and k are relatively prime positive integers and $n = h + k$. Show that for each j there are $h^{-1}\binom{n-1}{k}$ k-element subsets of $\{1, 2, \ldots, n-1\}$ with sum congruent to j modulo h.

Solution by Richard Holzsager, American University, Washington, DC. We transform the problem slightly. For each k-element subset $A = \{a_1, \ldots, a_k\}$ of $\{1, \ldots, n-1\}$, labeled so that $a_1 < \cdots < a_k$, define a k-element sequence $f(A) = (b_1, \ldots, b_k)$ by $b_i = a_i - i$ for $1 \leq i \leq k$. Then $0 \leq b_1 \leq \cdots \leq b_k \leq h - 1$, and f is a bijection between the subsets and the nondecreasing k-element sequences bounded between 0 and $h - 1$. Since we have reduced the sum of each set by a fixed amount $(k(k+1)/2)$, it suffices to show that the number of sequences with sum congruent to j mod h is independent of j.

Consider such a sequence B. If we replace each $b_i \in B$ by $b_i + 1 \bmod h$, then we add k to the sum. If $b_k = h - 1$, then to remain in the specified set of sequences we must also replace h's by 0's (and cyclically reorder), which does not change the sum modulo h. Since k is relatively prime to h, applying this injection h times leads us back to the original set through all the congruence classes modulo h, so each contains the same number of sequences.

Editorial comment. The proposer and the Anchorage Math Solutions Group applied a similar cyclic rotation to the original sets, viewed as subsets of an n-element set. Reiner Martin applied the properties of the q-nomial coefficient.

Solved also by G. Calinescu (Romania), R.J. Chapman (U.K.), M. Dindos (Slovakia), R. Martin (student), the Anchorage Math Solutions Group, and the proposer.

A Ratio with a Cauchy Distribution

10189 [1992, 60]. *Proposed by Ignacy I. Kotlarski, Oklahoma State University, Stillwater, OK.*

Suppose (X_1, X_2) and Y are two independent absolutely continuous random variables, where (X_1, X_2) has a distribution depending only on $X_1^2 + X_2^2$ and Y has an arbitrary distribution. Let $Z = (X_1 - X_2Y)/(X_1Y + X_2)$. Show that Z has a Cauchy distribution.

Solution by Kenneth Schilling, University of Michigan, Flint, MI. For $r > 0$, let $g(r)$ be the density of (X_1, X_2) at a point (x_1, x_2) with $x_1^2 + x_2^2 = r^2$. By changing to a form of polar coordinates, $X_1 = R\sin\Theta$ and $X_2 = R\cos\Theta$ with $-\pi \le \Theta \le \pi$, we have

$$P(\theta_1 < \Theta < \theta_2) = \int_{\theta_1}^{\theta_2}\int_0^{\infty} rg(r)\,dr\,d\theta = \frac{\theta_2 - \theta_1}{2\pi}.$$

Thus Θ is uniform on $(-\pi, \pi)$, so that $\tan\Theta$ is a Cauchy random variable.

Now let $\Phi = \arctan Y$ (so that Φ is a random variable on $(-\pi/2, \pi/2)$). Then $Z = \tan(\Theta + \Phi)$.

For any fixed real number ϕ, $\Theta + \phi$ is uniformly distributed modulo π. Hence, for fixed real numbers a and b,

$$P(a < \tan(\Theta + \phi) < b) = P(a < \tan(\Theta) < b).$$

Since Θ and Φ are independent, we have

$$\begin{aligned} P(a < Z < b) &= P(a < \tan(\Theta + \Phi) < b) \\ &= \int_{-\pi/2}^{\pi/2} P(a < \tan(\Theta + \phi) < b)\,dF_{\Phi}(\phi) \\ &= P(a < \tan\Theta < b) \end{aligned}$$

and so Z has a Cauchy distribution.

Editorial comment. Most solvers used a similar argument, and many noted that the absolute continuity if Y is irrelevant. José Luis Palacios employed a result from B. C. Arnold and P. L. Brockett, "On distributions whose component ratios are Cauchy", *The American Statistician*, 46 (1992), 25–26, and Gérard Letac

referred to G. Letac, "Which functions preserve Cauchy laws", *Proc. Amer. Math. Soc.*, 67 (1977), 277–286 and G. Letac, "Isotropy and sphericity: some characterizations of the normal distribution", *Annals of Statist.*, 9 (1981), 408–417 for more general work related to this problem.

Solved also by J. A. Bucklew, D. Callan, R. J. Chapman (U.K.), S. Gleason, E. Hertz, T. Hesterberg, N. Kang (student, Korea), K. S. Kedlaya (student), G. Letac (France), A. Nijenhuis, J. L. Palacios, D. M. Rosenblum, R. Stong, Anchorage Math Solutions Group, and the proposer. Two incomplete solutions were received.

An Interval of Differences

10190 [1992, 61]. *Proposed by Peter J. Ferraro, Roselle Park, NJ.*

Suppose t is a positive integer congruent to 1 modulo 4 but not a perfect square. Put $\alpha = (1 + \sqrt{t})/2$.

(a) Prove that if n is a positive integer, then

$$1 \le \lfloor \alpha^2 n \rfloor - \lfloor \alpha \lfloor \alpha n \rfloor \rfloor \le \lfloor \alpha \rfloor.$$

(b) Does every integer in the interval $[1, \lfloor \alpha \rfloor]$ occur as such a difference for some positive integer n.

Solutions by John Henry Steelman, Indiana University of Pennsylvania, Indiana, PA. We prove part (a) and show that the answer to part (b) is "yes". To get these results, let $\theta_n = \alpha n - \lfloor \alpha n \rfloor$. The one-dimensional case of Kronecker's theorem (due to Jacobi—see J. F. Koksma, *Diophantische Approximationen*, Springer, 1936, Theorem I.5, p. 10) shows that $\{\theta_n\}$ is dense in the interval $(0, 1)$ for irrational α.

Now let t and α be as in the statement of the problem. If $t = 1 + 4r$, then a straightforward calculation yields $\alpha^2 = \alpha + r$. Thus $\alpha^2 n = \alpha n + rn$ and hence $\lfloor \alpha^2 n \rfloor = \lfloor \alpha n \rfloor + rn$. It follows that

$$(\alpha - 1)\lfloor \alpha n \rfloor = (\alpha - 1)(\alpha n - \theta_n) = rn - (\alpha - 1)\theta_n.$$

Adding $\lfloor \alpha n \rfloor$ to each side of this equation yields

$$\alpha \lfloor \alpha n \rfloor = \lfloor \alpha n \rfloor + rn - (\alpha - 1)\theta_n = \lfloor \alpha^2 n \rfloor - (\alpha - 1)\theta_n.$$

Thus we conclude that $\{\lfloor \alpha^2 n \rfloor - \alpha \lfloor \alpha n \rfloor\}$ is dense in the interval $(0, \alpha - 1)$. As $\lfloor \alpha^2 n \rfloor - \lfloor \alpha \lfloor \alpha n \rfloor \rfloor = \lceil \lfloor \alpha^2 n \rfloor - \alpha \lfloor \alpha n \rfloor \rceil = \lceil (\alpha - 1)\theta_n \rceil$, we see that the set of such differences consists of those integers in the interval $[1, \lfloor \alpha \rfloor]$.

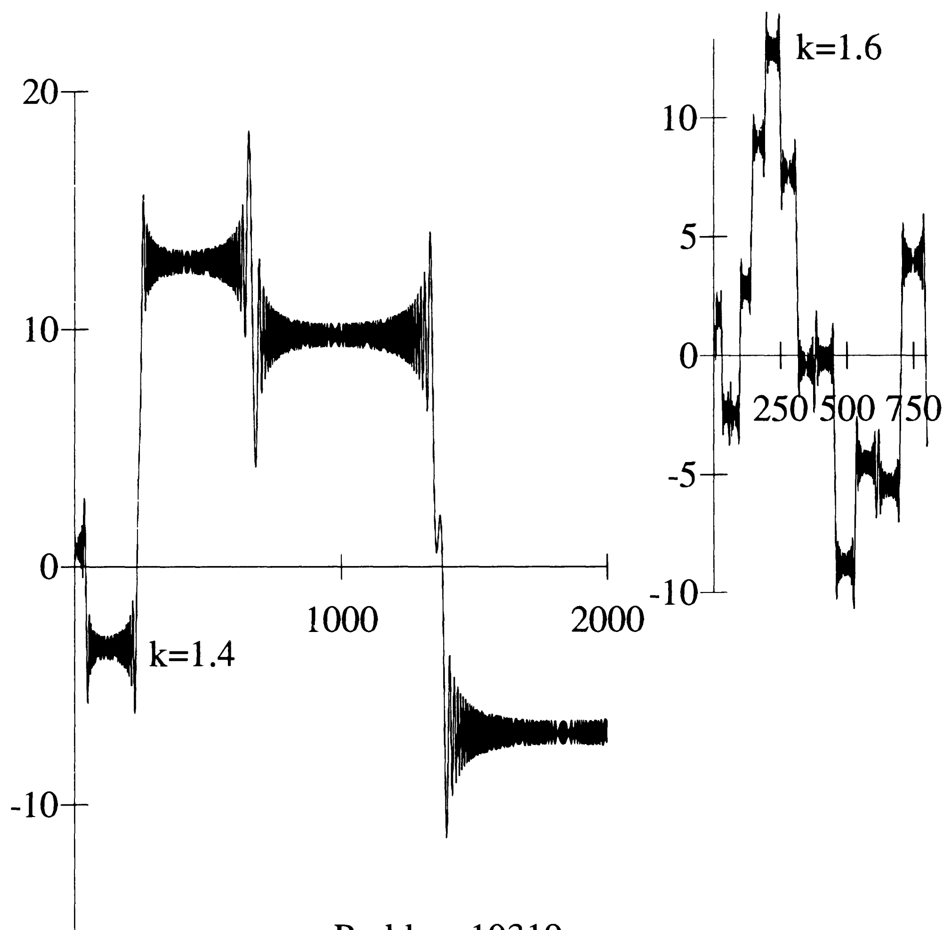
Solved also by D. Callan, R. J. Chapman (U.K.), J. Fukuta (Japan), B. Haible (Germany), R. Holzsager, K. S. Kedlaya (student), O. P. Lossers (The Netherlands), R. Stong, B. M. M. de Weger (The Netherlands), O. Wyler, University of South Alabama Problem Group, and the proposer.

Answer to Picture Puzzle:
(p. 488)

Both Ivan Niven and Lida Barrett have been president of the MAA.

The American Mathematical Monthly

Volume 100, Number 6 / JUNE–JULY 1993



Problem 10319

AN OFFICIAL PUBLICATION OF THE MATHEMATICAL ASSOCIATION OF AMERICA

NOTICE TO AUTHORS

The *Monthly* publishes articles, notes, and other features about mathematics and the profession. The readership of the *Monthly* is intended to include everybody who is mathematically inclined, including of course professional mathematicians and students of mathematics at all collegiate levels. While no single article or feature is likely to appeal to everyone, material should interest and be accessible to a large number of readers. This is the most important criterion for acceptance.

Articles may be expositions of old results or presentations of new ones. They may concern all of mathematics or one small area, a broad development or a single application, historical reminiscences or one important event. While some articles may contain the author's new research, the novelty of material and generality of the results is far less important than the clarity of exposition and general interest. Discussing one illuminating case of a well known result is far better than providing all the details of an obscure but new proposition. Articles in the *Monthly* are supposed to inform and to entertain; they are meant to be read rather than archived.

Notes are short and possibly informal articles. A note may concern a clever new proof of an old theorem, a novel way to present tired material, or a lively discussion of a philosophical (but still mathematical) issue. Also, any topic is suitable, so long as it is related to mathematics. Because a note is short, the first few sentences are the most important part: They should explain the purpose and invite the reader in. Photographs or diagrams often will attract the reader's attention.

All articles and notes should be sent to the editor:

JOHN EWING,
Department of Mathematics,
Indiana University,
Bloomington, IN 47405.

Please send 3 copies, typewritten on only one side of the paper. Illustrations should be carefully drawn on separate sheets of paper in black ink; the original should be without lettering and two copies should have appropriate captions and lettering indicated.

Proposed problems or solutions should be sent to:

RICHARD BUMBY,
P.O. Box 10971
New Brunswick, NJ 08906-0971.

Please send 2 copies of all material, typewritten if possible.

Letters to the Editor, both for publication and for private reading, should be sent to the Editor at the address given above. Comments, including criticisms, are welcome, as are all suggestions for making the *Monthly* a lively, entertaining, and informative journal.

Reprint permission:
MARCIA P. SWARD, Executive Director

Advertising Correspondence:
Ms. ELAINE PEDREIRA, Advertising Manager

Subscription correspondence, change of address, and other inquiries:
Membership / Subscriptions Department

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036.

Microfilm Editions: University Microfilms International, Serial Bid coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

The AMERICAN MATHEMATICAL MONTHLY (ISSN 0002-9890) is published monthly except bimonthly June-July and August-September by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, DC 20036 and Montpelier, VT. Second class postage paid at Washington, DC, and additional mailing offices. ***Postmaster***: Send address changes to the American Mathematical Monthly, Membership / Subscription Department, MAA, 1529 Eighteenth Street, N.W., Washington, DC, 20036-1385.

The American
Mathematical Monthly

Volume 100, Number 6 / JUNE–JULY 1993
(ISSN 0002-9890)

Contents

ARTICLES

FEATURES

Thomas Archer Hirst—Mathematician Xtravagant II. Student Days in Germany

J. Helen Gardner and Robin J. Wilson

> Yesterday evening about 30 members of the Halifax Mechanics Institute and Mutual Improvement Society took tea together at Stott's Temperance Hotel, Broad Street, for the purpose of presenting a testimonial of respect to Mr Thomas A. Hirst, assistant to Mr Carter, land surveyor, who is about leaving the town. Mr Hirst has been an active voluntary teacher in the above society for upwards of $3\frac{1}{2}$ years, and has won the esteem and respect both of the directors and members, especially those of his own class, having taught the higher branches of mathematics with great ability.

After completing his apprenticeship on 31st August 1850, Thomas Hirst "bid adieu to surveying" forever. Remembering his earlier brief visit to Germany, and attracted by John Tyndall's enthusiasm for the University of Marburg, he resolved to study there. Tyndall was about to return to Marburg, and so Hirst went with him, arriving on 10th October after a delightful three-day journey visiting the Rhine.

Hirst quickly established for himself a daily routine which combined studying the German language with indulging his love of literature and pursuing his various scientific activities:

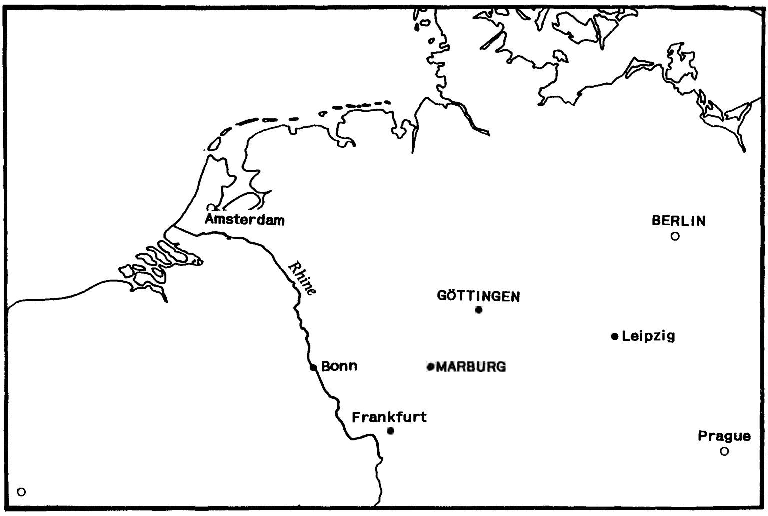
> **18th October 1850:** . . . My time is divided thus:- I rise and get my breakfast eaten before 8 a.m. then smoke a cigar and begin the day by one of those fast earth-bound unenthusiastic essays of Montaigne. This I do medicinally to discipline myself for the practical labours of the day, then from 9 to near 1 p.m. I work in the laboratory . . . Dinner, and afterwards German translation until dusk ($5\frac{1}{2}$), then a walk until lamp time, then German again (with an interval for tea) until $9\frac{1}{2}$; from that time to 10 my journal occupies me generally, and from 10 to 10.30 as I said Tyndall and I sweeten the day's labour with a poem.

Hirst matriculated at the University on 2nd November 1850. Being uncertain of the exact direction which his studies should take, he decided to pursue the three sciences of chemistry, physics and mathematics. His hope was that, by attending lectures in these areas, he would be able to "make choice which of the three should form the subject of my future and more particular study".

Just as Tyndall had done previously, he attended the lectures of Robert Bunsen on chemistry, Christian Gerling on physics, and Friedrich Stegmann on mathematics. He was most enthusiastic about a laboratory session of Bunsen, but seemed rather less enthusiastic about the lectures of the other two:

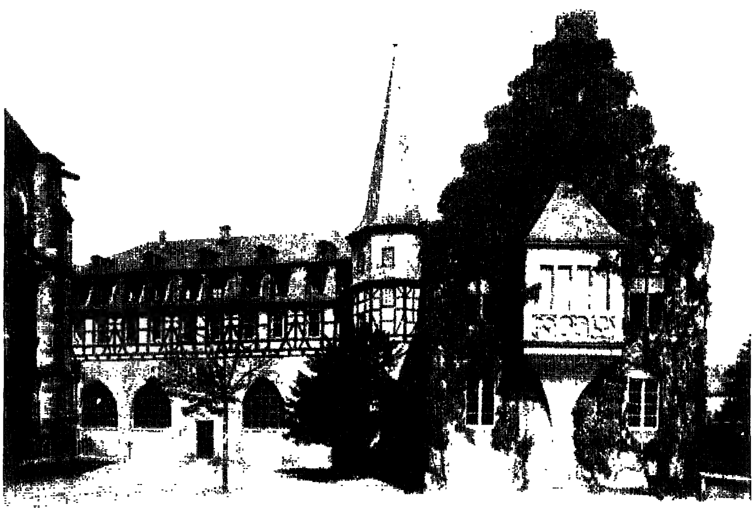
> **5th November 1850:** . . . From 9 to 12 at laboratory. All the students began their practical course, the lectures don't commence until Thursday. Bunsen however, was present all the time and moved about from one to another, in a way that does one's heart good; able man as he is everywhere acknowledged to be, there is not the least spark of pride in him, his disposition

Map of Germany
showing Marburg, Göttingen, and Berlin



Tyndall's description of the University

Our University is not grand, it is broken into parts and presents no imposing front. Our laboratory presents rather a scoundrel-like appearance, but don't conclude hastily against it—it holds a man [Bunsen] whose superior as a chemist is not to be found within a radius of 8000 miles from the Piece Hall of Halifax. There, however, right over against me on the summit of a hill, with the sun shining upon its white walls, and its tower piercing the air, is a fine building—an astronomical observatory and physical institute, its interior furnished with costly apparatus; on the other hand I can lead you into a little room with hacked rickety benches, perhaps the whole not worth five and sixpence, where a man of genius makes his hearers forget the poorness of his furniture, as he crushes the crust of a mathematical calculation between his fingers.



which shines through his face is a model of gentleness, geniality and integrity and humility, he is universally beloved here, and in his presence all feel at home and encouraged.

12 to 1 with Gerling. He is an old man with a good deal of the pedant about him, of weak concentrative intellect, and as is usual too much vanity. With all that however, he is what is generally called a good-hearted old boy.

From 3 to 4 with Stegmann who differs again materially from the rest. His appearance is not prepossessing, he is an ordinary looking little man with however, a sharp nose, pale studious face, and deep sunk eyes. He bolts into the room and into his mathematics at one and the same time, wasting no time either in prelude or wordy introduction. There is a figure chalked on his black-board almost before you are aware he is present, he talks in a slow distinct voice, carves his subject deliberately piecemeal and at his exit as at his entrance you are just considering and in the middle of his last equation when you find that he has bolted, shut the door and not a vestige even of his coat flap is visible. The idea presents itself to you that if you were to follow him the moment you missed him, you would find him buried in a mathematical problem in his own room. When you come to know him, however, you find him a thorough good fellow, who always pretends less than he intends performing.

Daily his German became more fluent and his understanding more reliable. His attendance at lectures helped with this, and by mid-November Hirst began to notice the improvement himself:

19th November 1850: ...I find that with Stegmann I am learning more German than with any other. He reads mathematical operations for us to copy in writing. At first I could not copy a word, then occurred a space of time when most terrible and exasperating blanks occurred. Now only a few blanks in a page perhaps...

The turn of the year showed that Hirst had, as earlier in Halifax, quickly settled himself comfortably into a new community, and by the Spring he felt quite at home. It came as a great disappointment when Bunsen announced his impending departure from Marburg:

5th April 1851:...Bunsen called on me. He is a kind fellow indeed, during the last 2 months I have been working at the quantitative analysis of some minerals from Iceland, and he has been at great pains in explaining a theory of his as to their formation, by which theory the calculated and analysed composition shew a remarkable agreement. My analyses are a further proof of the veracity of his law, and he, thinking that some publicity would be of service and acceptable to me, proposed to me to write a small notice of my analyses and calculations for "Liebig's *Annalen*"; nay more in spite of his extreme business just now as in 2 or 3 days he leaves Marburg he has sketched out an article and to-day brought it to me. As to my share in the investigation it has been so commonplace that I should certainly refuse to publish any such article. Viewed, however, as a corroboration of *his* work, it will extend the speed of his researches and so I do it. As for the kindness tome, it was well meant, though if he knew me better he would not have offered it.

Robert Bunsen (1811–1899)

He increasingly gained satisfaction from his mathematical work, frequently to the detriment of his other subjects:

15th June 1851: ...I could do nothing well but mathematics, this week. Physics or chemistry or general literature were as arrows, that could find no entrance through my mathematical coat of mail, but glanced off merely...

Never content to relax, he worked up to sixteen hours a day, and this soon began to affect his health. Overwork and lack of physical exercise began to cause intestinal problems that were to affect him throughout his life, and he suffered an attack of dropsy. His dissatisfaction with his life style, and his frustration with his lack of progress, frequently spill over into the pages of his diaries.

27th July 1851: Many a time this week have I cursed this inward shrinking at intellectual obstacles, subjects pass by me skimmed, not penetrated into; and in spite of the day's proper number of hours having been devoted to one's task, at their close is no satisfaction. Sometimes I cry to myself, "Is it not possible to get thyself absorbed in thy work, Tom—fully?" and if not, "Is success possible?" To which I can but answer, "Thy Duty is to *do* thy work, with or without absorption therein; therefore, go about it instantly." Patience, therefore, more energetic work, and action is my need. Then from the feeling of recreation *earned*, the latter also will react on health and strength. At present my work and recreation are both accompanied with too little physical exercise. *That*, therefore, is the point to be attacked.

His life style even affected his social activities:

10th August 1851: On Tuesday evening at Museum, at a ball in the gardens. The night was chill, I dropped too suddenly from Differential Calculus into ladies' society, and could not give myself freely to the change. After an hour's unsuccessful attempt so to do, I returned, cursing the mode of life I was pursuing; next morning I had already shaken hands, however, with Diff. Calculus, and forgot the ladies...

He found relaxation in reading Tennyson and Carlyle, and translating into English the works of Goethe and Schiller:

12th October 1851: My days have been thus divided: up at 7, breakfast and Schiller until 8, then mathematics until 12.30, a walk from that time to 1, then dinner and Schiller or 'Leader' until 2.30. Once more mathematics until 5, then Physics until 7; from 7 to 8 tea and Schiller, from 8 to 11 translations of Schiller, from 11 to 12 cigar and Schiller, then to bed.

It was around this time that the direction of his future studies began to emerge more clearly. Believing that "if the heart is not in the work, there is poor chance either of success therein, or of steady perseverance", he found the idea of concentrating on mathematics increasingly compelling:

14th December 1851: ...After waverings and experiments every day brings with it the stronger conviction that my labour, in which I must find my daily discipline and duty, must be in the mathematical field. Many a time have I asked myself "what then is the absolute value of being expert at addition and subtraction? Did I come into the world to be an animated Ready-reckoner merely?" Such questions occur daily more seldom, dim visions of a higher destiny have long floated before me, as God forbid they should ever cease to do. But they *have* brought with them heretofore not merely a disturbance of the concentration necessary bravely to fulfil the day's duty, but also scattered energy to fulfil any work and even a morbid depreciation as to the value of all work itself. These dim visions of a higher density are like too full sails—dangerous, when the proportionate ballast is not there... I begin to get a gleam that there is a higher value in the multiplication table than that which teaches us that twice two make four. The Ready-reckoner even may have its transcendent side...

Life by now was incomparably better than it had been, although festivals were still

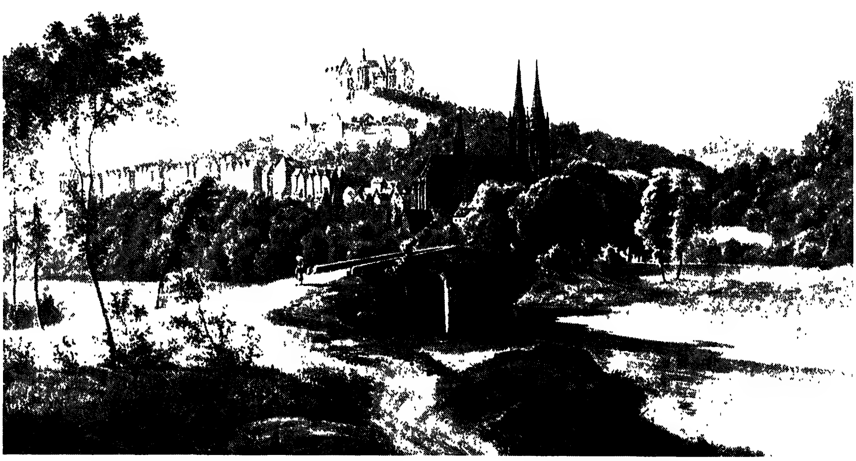
celebrated with his books, and social occasions were usually overshadowed by work:

28th December 1851: A different Christmas to any I ever spent before has again passed by. This time I had no one to share it with except Brandes Analyt: Geom: and Boucharlat's Mechanics, both which, however, if not merry, were at least interesting companions.

31st December 1851: To-night there is a ball in the Ritter. I am seated at my table at the window investigating the properties of an Ellipsoid. The music comes across the Ketzerback, mellowed by the gusts of wind—it is as if Nature had turned my room into a flute and breathed soothing harmony through it. All this serves as an accompaniment, almost unconsciously so, to my work. I have not been out for two or three days, and not the slightest idea that the New Year was on the threshold and the Old Year nearly dead: when suddenly my neighbour St Elizabeth announces the fact by tolling 12 times—simultaneously outside, where all was before in stillness, the air rings with cries of "Prost Neu Jahr!" ... My pen fell from my hand, and the whole past year stood before me with wondrous vividness. It has been an eventful one to me—filled with manifold new and instructive experiences. More foothold I do possess than before, so hail to thee, New Year. "Have at you," as boxers would say.

Hirst's description of Marburg

... Marburg stands on the inner apex of an acute angle in the Lahn valley, which is a river running nearly North and South to the Rhine. Marburg stands then on the west bank, and the river flows past it with a graceful sweep into a quiescent broad hill-encircled valley to the South. It was near sunset, with a beautiful sky and a wind just strong enough to make the dying leaves sing musically and take their last and only flight high into the air before they sunk to their final rest... Immediately before us was Augusta's Ruhe and a little farther Marburg Castle on hills of about equal height their slopes carefully terraced into rich looking gardens. To the west the sun was sinking behind the far distant purple hill between which and us was the most graceful alternation of hills and valleys with their red fallows, green, beautiful green meadows and brown woods. The spires of the church rose tapering in calm religious ascension, and the grand old castle, looked over all, with its most resigned and reverend glance. Marburg thou art indeed set in the midst of a fairy land!



By March 1852, he was completely at home in Marburg, commenting that "Germany and Germans are now to me as a native land and brothers, whereas the year

before there was ever a feeling of strangeness present". He had determined to complete his studies there during the vacation, but a letter from John Tyndall changed his plans entirely.

> **1st March 1852:** ... An unconscious notion possessed me before that haste was needed and that it was time I left Germany. How the notion came I know not. True it is, however, when John said if he were in my place he would be in no haste the idea struck me as new, and in an hour I had made other plans, namely quite silently and unknown to any of them I will walk in and visit England, and as quickly and quietly return to Berlin or Göttingen at the beginning of next Semester. This arrangement will give me an opportunity to proceed far further with my Mathematics, and to hear some of the first German mathematicians; after which time I may sit down more confidently to a dissertation...

However, Stegmann advised him to take his oral examination before leaving for home and then to return to complete his written dissertation. His oral examination took place on 16th March 1852, and covered physics (the motion of a pendulum, acoustics and light), crystallography and chemistry, and mathematics. It is interesting to note the areas covered by a mathematics student at that time:

> ...we went through part of the theory of Equations, namely the solution of general and numerical equations of higher powers—also the principal methods of elimination with two or more unknown terms. From this he turned to the theory of Curved Surfaces, principally on the Tangential Plane and Euler's Law of Curvature. He did not ask a single question in Differential or Integral Calculus, for which I was sorry. Instead of that, he asked finally a question in Descriptive Geometry, for which I was not so well prepared... After a close examination of two hours, however, I was ordered to retire and in a few minutes was recalled, when the Decan told me they were satisfied, and that as soon as the necessary dissertation was approved I should receive my Degree...

He could now prepare for his brief visit to England.

> **17th March 1852:** After packing up my traps I went round to say good-bye to Professors and friends. Congratulations met me on every hand. They were mostly sincere, too, and as I had earned them I received them willingly. Shortly before dusk I took a walk towards Wertha, as I did yesterday evening before my examination. Then to prepare myself for the coming trial—now to cogitate on my past year and a half's work... Another phase of my life is concluded, and thank God, it is an improvement on the foregoing. Here, however, it must not and shall not rest —it is but the beginning of new and better directed activities...

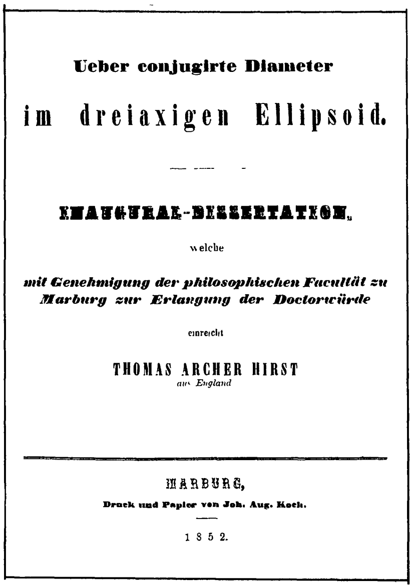
After returning to Marburg, he began work on his Ph.D. dissertation, "On conjugate diameters of the triaxial ellipsoid". By mid-June, he was able to write:

> **13th June 1852:** ... the neck of my dissertation is already broken. Last Christmas, as I told you, I looked round the matter and spent the last part of a week thereon. Since I returned from England I have stuck pretty closely to it for ten days, and it is now done. The thing is small, it is true, but I have Stegmann and Schell's authority when I say it is a neat little investigation; both of them kindly offered to give me any assistance they could, but I did not require it...

However, it was not all plain sailing. In particular, he had a lot of trouble trying to simplify one complicated, but important, expression. Even Wilhelm Schell, his "quick, brilliant and impulsive" supervisor, was unable to help. But a few days later, Hirst was successful:

> One morning at 5 a.m. in bed a thought struck me in reference to this identical expression, to interpret whose significance had baffled me for two days. Acting on the hint, I got up, washed

myself from top to toe, and walked into it until dinner time. It was one of the luckiest hints that ever came to me—obstacle after obstacle tumbled before it, and in two days after the whole problem, much to my surprise as well as that of Stegmann and Schell, was solved. The same day Stegmann came to sit an hour with me, not having seen me for more than a week. 'How do you get on with the Dissertation?' he asked. 'I think I have done it, Professor,' I replied. He put on one of his half sarcastic, half sceptical smiles, and asked me to shew him it. I did so. He made no remark at all, until I had finished—then from his countenance one could scarcely interpret an approval—the careful dog—He then called me back very pertinently to a few important parts I had explained badly: and at length expressed his entire satisfaction saying he could suggest no improvement. I have just translated it into German roughly, and Schell is kindly correcting it for me...


Ueber conjugirte Diameter

im dreiaxigen Ellipsoid.

Inaugural-Dissertation,

welche

mit Genehmigung der philosophischen Facultät zu Marburg zur Erlangung der Doctorwürde

einreicht

THOMAS ARCHER HIRST
aus England

Marburg,
Druck und Papier von Joh. Aug. Koch.

1852.

Thomas Hirst's Ph.D. dissertation
"On conjugate diameters of the triaxial ellipsoid"

The dissertation was quickly approved, and Hirst was awarded his doctorate in July 1852. Like his friend Tyndall, he had completed his studies within two years, instead of the usual three.

3rd July 1852: I received orders to-day to attend upon the University Decan, Prof. Bergk, which I obeyed. It was to tell me that my dissertation had been approved of by the Philosophical Faculty, and upon delivering 120 printed copies to the University I should receive my Diploma. I took the MS. therefore, immediately to Printer Kock.

I learnt afterwards from Professor Stegmann that it first went to Prof. Gerling and his written opinion on the accompanying form was to the effect: "I find the dissertation good, and have only a few suggestions with respect to order and other trivial matters to make; I think it, however, advisable for Prof. Stegmann to certify publicly that *Mr Hirst has made it without his help*"!!! The poor old fellow, I suppose, felt slighted that after hearing his lectures on Trigonometry I declined making him my mathematical tutor. Stegmann certified accordingly that the dissertation was completed before he saw it—indeed, he might have added that he was not in Marburg when it was written.

I have received an invitation to become a member of the Mathematical Kräntzchen [circle] with Professors Stegmann, Gerling, Hessel, etc. Doctors Kohlrausch, Schell, etc. to be held weekly in the open air.

11th July 1852: On Monday evening I attended the Mathematical Kräntzchen in Prof. Hessel's garden. It is an interesting meeting indeed. Stegmann, with his keen intellect and quiet sarcasm, Gerling with intense vanity and essential insignificance, Hessel with his reserve and stubborn gruffness, and Schell with his unpretending, brilliant suggestions make by their contrast an interesting study...

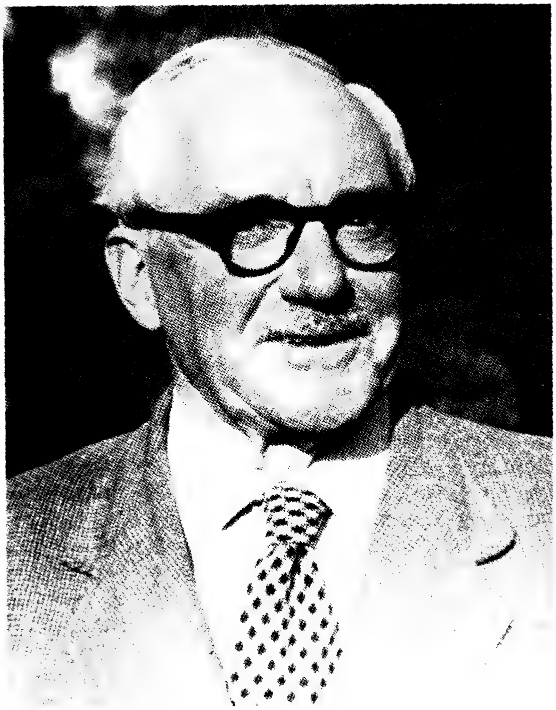
For some time Hirst had resolved to visit Göttingen and Berlin to learn from the greatest German mathematicians of the day. In the former, he would work on magnetic experiments with Weber, and visit Gauss; in the latter, where he was to spend the winter semester, he would become a good friend of both Dirichlet and Steiner. His account of this exciting time in his life forms the topic of the next article.

ACKNOWLEDGMENTS. A typed version of the Thomas Hirst diaries is held at the Royal Institution in London, and quotations from the diaries appear here by courtesy of the Royal Institution. The diaries have been edited by W. H. Brock and R. M. MacLeod, and were published in microfiche by Mansell, London, in 1980.

Open University
Milton Keynes MK7 6AA
England

PICTURE PUZZLE

(from the collection of Paul Halmos)



"Is he hardier than a small forest?

(see page 596)

How To Make Wavelets

Robert S. Strichartz

§1. INTRODUCTION. The French call them *ondelettes*, these new high-tech gadgets in the arsenal of harmonic analysis. Move over, Fourier! Your series and transforms are not the only game in town. Wavelet expansions enjoy a number of good properties not available in other types of expansions. To see this in the simplest context, consider a real-valued function $f(x)$ on the interval $[0,1]$. You can expand it in a Fourier series

$$f(x) = b_0 + \sum_{1}^{\infty} (b_k \cos 2\pi kx + a_k \sin 2\pi kx) \tag{1.1}$$

or you can expand it in a Haar function series

$$f(x) = c_0 + \sum_{j=0}^{\infty} \sum_{k=0}^{2^j-1} c_{jk} \psi(2^j x - k) \tag{1.2}$$

where $\psi(x)$ is the function defined by

$$\psi(x) = \begin{cases} 1 & \text{if } 0 \le x < \frac{1}{2} \\ -1 & \text{if } \frac{1}{2} \le x < 1 \\ 0 & \text{otherwise.} \end{cases} \tag{1.3}$$

(see FIGURE 1).

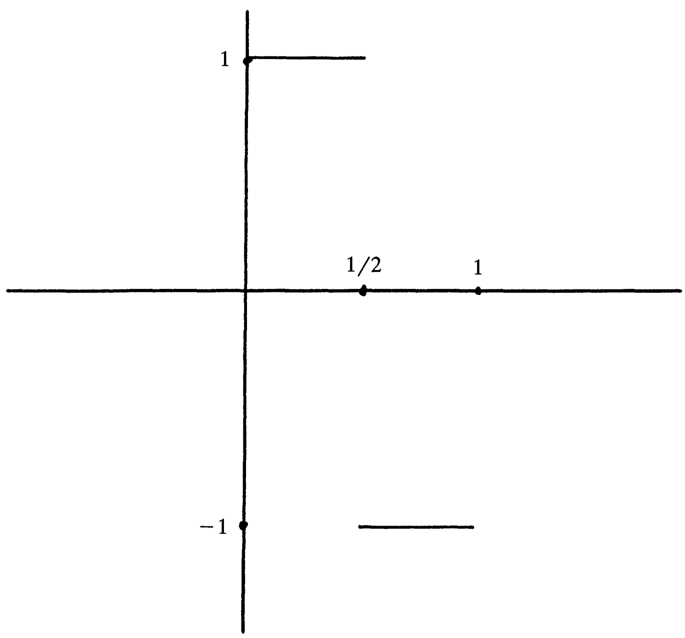


Figure 1. The graph of the generator of the Haar functions.

Both series are examples of expansions in terms of orthogonal functions in $L^2(0,1)$. Thus there are simple formulas for the coefficients. (Exercise: Show that $\{\psi(2^j x - k)\}$ are orthogonal, but not normalized.) But the Fourier series is not well localized in space; if you are interested in the behavior of $f(x)$ on a subinterval $[a,b]$ you need to involve all the Fourier coefficients. On the other hand, the Haar series is very well localized in that to restrict attention to the subinterval $[a,b]$ you need only take the sum in (1.2) over those indices for which the interval $I_{jk} = [2^{-j}k, 2^{-j}(k+1)]$ (the support of $\psi(2^j x - k)$) intersects $[a,b]$. Furthermore, the partial sums of the Haar series (summing $0 \le j \le N$) clearly represents an approximation to f taking into account details on the order of magnitude 2^{-N} or greater. These two properties, *localization in space*, and *scaling*, are the hallmarks of wavelet expansions. In addition, the Haar functions are created out of a single function ψ by dyadic dilations and integer translations. Essentially the same property is shared by all the wavelet bases we will discuss, and may in fact be taken as an approximate definition of a wavelet expansion.

The wavelet expansions we are going to construct can be thought of as generalizations of the Haar series, in which the function ψ is replaced by smoother cousins. Before we can say exactly what properties we want these functions to have, and how we can go about constructing them, it is useful to backtrack and see exactly how the Haar functions arise. It will turn out to be easier if we consider the whole line as the domain of our functions.

§2. THE ROUGH-AND-READY HAAR WAVELETS. We begin with the function φ = characteristic function of the unit interval $[0,1]$. Surely this is one of the simplest functions one can imagine, but it is chosen because it has two important properties:

(i) the translates of φ by integers, $\varphi(x-k)$, $k \in \mathbb{Z}$, form an orthonormal set of functions for $L^2(\mathbb{R})$;

(ii) φ is *self-similar*. If you cut the graph in half then each half can be expanded to recover the whole graph. This property can be expressed algebraically by the *scaling identity*

$$\varphi(x) = \varphi(2x) + \varphi(2x-1). \tag{2.1}$$

We will call φ the *scaling* function. (In the French literature it is sometimes called "le père" and ψ is called "la mère," but this shows a scandalous misunderstanding of human reproduction; in fact the generation of wavelets more closely resembles the reproductive life style of an amoeba.) In fact, the scaling identity essentially determines φ up to a constant multiple (exercise). The significance of the scaling identity is the following: Let V_0 denote the linear span of the functions $\varphi(x-k)$, $k \in \mathbb{Z}$ (or by abuse of notation the closure in $L^2(\mathbb{R})$ of this span, $\sum_{k=-\infty}^{\infty} a_k \varphi(x-k)$ with $\sum |a_k|^2 < \infty$). This is a natural space to consider in view of (i), since the functions $\varphi(x-k)$ form an orthonormal basis for V_0. Of course V_0 is not all of L^2, it is the subspace of piecewise constant functions with jump discontinuities at $\mathbb{Z}$. We can get a larger space by rescaling. Let $(1/2)\mathbb{Z}$ denote the lattice of half-integers $k/2$, $k \in \mathbb{Z}$, and let V_1 denote the subspace of L^2 of piecewise constant functions with jumps at $(1/2)\mathbb{Z}$. It is clear that $f(x) \in V_0$ if and only if $f(2x) \in V_1$, and the functions $2^{1/2}\varphi(2x-k)$ form an orthonormal basis for V_1 (the factor $2^{1/2}$ is thrown in to make the normalization $\|2^{1/2}\varphi(2x-k)\|_2 = 1$ hold). The scaling identity (2.1), or rather its translated version

$$\varphi(x-k) = \varphi(2x-2k) + \varphi(2x-2k-1) \tag{2.1$'$}$$

says exactly $V_0 \subseteq V_1$, since a basis for V_0 is explicitly represented as linear combinations of basis elements of V_1. (Of course the containment $V_0 \subseteq V_1$ is clear from the description of the spaces V_0 and V_1 in terms of locations of jump discontinuities, but in the generalizations to come there will be no such simple description; however, there will be a scaling identity.)

The whole story can now be iterated, both up and down the dyadic scale. The result is an increasing sequence of subspaces V_j for $j \in \mathbb{Z}$, where V_j consists of the piecewise constant L^2 functions with jumps at $2^{-j}\mathbb{Z}$, and the functions $2^{j/2}\varphi(2^j x - k)$ for $k \in \mathbb{Z}$ form an orthonormal basis for V_j. We can pass back and forth among the space V_j by rescaling: $f(x) \in V_j$ if and only if $f(2^{k-j}x) \in V_k$, and the scaling identity (2.1), suitably rescaled, says $V_j \subseteq V_k$ if $j \leq k$. The sequence $\{V_j\}$ is an example of what is called a *multiresolution analysis*. There are two other properties of $\{V_j\}$ that are significant, namely

$$\bigcap_{j \in \mathbb{Z}} V_j = \{0\}, \tag{2.2}$$

and

$$\bigcup_{j \in \mathbb{Z}} V_j \text{ is dense in } L^2 \tag{2.3}$$

(exercise).

In view of (2.3) it would seem tempting to try to combine all the orthonormal bases $\{2^{j/2}\varphi(2^j x - k)\}$ of V_j into one orthonormal basis for $L^2(\mathbb{R})$. But look, although $V_j \subseteq V_{j+1}$, the orthonormal basis $\{2^{j/2}\varphi(2^j x - k)\}$ for V_j is not contained in the orthonormal basis $\{2^{(j+1)/2}\varphi(2^{j+1}x - k)\}$ for V_{j+1}. (Indeed, there are distinct elements in the two orthonormal bases that are not orthogonal to each other.) So our first naive attempt to obtain an orthonormal basis for $L^2(\mathbb{R})$ is flawed. Can we fix it up?

Back to the drawing boards! Since $V_0 \subseteq V_1$ and we have an orthonormal basis for V_0 of the form $\{\varphi(x - k)\}$, why don't we try to complete an orthonormal basis of V_1 by adjoining functions of the form $\{\psi(x - k)\}$ for some function ψ? This is the same thing as asking for an orthonormal basis of the desired form for the orthogonal complement of V_0 in V_1, which we denote W_0, so $V_1 = V_0 \oplus W_0$ (Hilbert space direct sum).

The answer is easy: we want to take ψ exactly to be the Haar function generator defined in §1. Note that ψ can be expressed in terms of φ by

$$\psi(x) = \varphi(2x) - \varphi(2x - 1) \tag{2.4}$$

which is very reminiscent of the scaling identity. Exercise: show that $\{\psi(x - k)\}$ forms an orthonormal basis for W_0. But now we can rescale the space W_0, so

$$V_{j+1} = V_j \oplus W_j \tag{2.5}$$

and $\{2^{j/2}\psi(2^j x - k)\}_{k \in \mathbb{Z}}$ is an orthonormal basis for W_j. If we combine conditions (2.2), (2.3) and (2.5) we obtain

$$L^2(\mathbb{R}) = \bigoplus_{j=-\infty}^{\infty} W_j \tag{2.6}$$

and since the spaces W_j are all mutually orthogonal we can now refine our naive

attempt and combine all the orthonormal bases for W_j into one grand orthonormal basis $\{2^{j/2}\psi(2^j x - k)\}_{j\in\mathbb{Z},\ k\in\mathbb{Z}}$ for $L^2(\mathbb{R})$. (The only change is that we have replaced the scaling function φ by the wavelet ψ.) This gives the Haar series basis for the whole line. There is a minor variation on this theme that is perhaps more closely related to the Haar expansion on the unit interval: instead of (2.6) we can also write

$$L^2(\mathbb{R}) = V_0 \oplus \left(\bigoplus_{j=0}^{\infty} W_j \right) \tag{2.6$'$}$$

and then combine the basis $\{\varphi(x-k)\}_{k\in\mathbb{Z}}$ for V_0 with the bases $\{2^{j/2}\psi(2^{1/2}x - k)\}_{k\in\mathbb{Z}}$ for W_j with $j \geq 0$, to obtain an orthonormal basis for $L^2(\mathbb{R})$.

§3. MULTIRESOLUTION ANALYSIS. The moral of the story so far is that we first want to build a scaling function φ and associated multiresolution analysis $\cdots \subseteq V_{-1} \subseteq V_0 \subseteq V_1 \subseteq \cdots$ before constructing the wavelets.

Definition. A *multiresolution analysis* $\cdots \subseteq V_{-1} \subseteq V_0 \subseteq V_1 \subseteq \cdots$ with scaling function φ is an increasing sequence of subspaces of $L^2(\mathbb{R})$ satisfying the following four conditions:

(i) (density) $\bigcup_j V_j$ is dense in $L^2(\mathbb{R})$,
(ii) (separation) $\bigcap_j V_j = \{0\}$,
(iii) (scaling) $f(x) \in V_j \Leftrightarrow f(2^{-j}x) \in V_0$
(iv) (orthonormality) $\{\varphi(x-k)\}_{\gamma\in\mathbb{Z}}$ is an orthonormal basis for V_0.

It follows easily from the definition that $\{2^{j/2}\varphi(2^j x - \gamma)\}_{\gamma\in\mathbb{Z}}$ forms an orthonormal basis for V_j. Since $\varphi \in V_0 \subseteq V_1$ we must have

$$\varphi(x) = \sum_{\gamma\in\mathbb{Z}} a(\gamma)\varphi(2x-\gamma) \tag{3.1}$$

for some coefficients $a(\gamma)$ satisfying

$$\sum_{\gamma\in\mathbb{Z}} |a(\gamma)|^2 = 2 \tag{3.2}$$

and in fact

$$a(\gamma) = 2\int \varphi(x)\overline{\varphi(2x-\gamma)}\,dx. \tag{3.3}$$

Equation (3.1) is the analogue of (2.1), and we will refer to it as the *scaling identity*.

It follows from the definition that the scaling function determines the multiresolution analysis, but not conversely. A more difficult question is how to characterize those functions φ which are scaling functions for a multiresolution analysis. Here we expect the scaling identity to play a crucial role, but before we can say more we need to examine certain algebraic conditions on the coefficients $a(\gamma)$ that follow from the definition.

First, there is a consistency condition that arises from (iv) and (3.1). We know from (iv) that

$$\int \varphi(x-\gamma)\overline{\varphi(x)}\,dx = \delta(\gamma, 0) \tag{3.4}$$

(Kronecker δ). If we use (3.1) to substitute for $\varphi(x-\gamma)$ and $\overline{\varphi(x)}$ in (3.4) we

obtain

$$\sum_{\gamma'\in\mathbb{Z}}\sum_{\gamma''\in\mathbb{Z}} a(\gamma')\overline{a(\gamma'')}\int\varphi(2x-2\gamma-\gamma')\overline{\varphi(2x-\gamma'')}\,dx$$

$$= 2^{-1}\sum_{\gamma''=2\gamma+\gamma'}\sum a(\gamma')\overline{a(\gamma'')} = \delta(\gamma,0)$$

after the change of variable $x \to 2^{-1}x$ and use of (3.4). We rewrite this as

$$\sum_{\gamma'\in\mathbb{Z}} a(\gamma')\overline{a(2\gamma+\gamma')} = 2\delta(\gamma,0). \tag{3.5}$$

Note that (3.5) contains (3.2) as a special case.

Another algebraic condition arises if we assume φ is integrable and $\int\varphi(x)\,dx \neq 0$ (if $\int\varphi(x)\,dx = 0$ then the same is true for all functions in all V_j, so we would not expect to have the density condition (i)). Then we integrate (3.1) and make a change of variable to obtain

$$\int\varphi(x)\,dx = \sum_{\gamma\in\mathbb{Z}} a(\gamma)\int\varphi(2x-\gamma)\,dx$$

$$= \sum_{\gamma\in\mathbb{Z}} a(\gamma)2^{-1}\int\varphi(x)\,dx$$

hence

$$\sum_{\gamma\in\mathbb{Z}} a(\gamma) = 2. \tag{3.6}$$

Now we would like to reverse the procedure. *Step 1* will be to produce solutions $a(\gamma)$ to the algebraic identities (3.5) and (3.6). *Step 2* will be to define the scaling function via the scaling identity (3.1). Notice that (3.1) says that φ is a fixed point of the linear transformation

$$Sf(x) = \sum_{\gamma\in\mathbb{Z}} a(\gamma)f(2x-\gamma) \tag{3.7}$$

so it is reasonable to try to construct φ by iterating S,

$$\varphi = \lim_{n\to\infty} S^n f \tag{3.8}$$

for some reasonable initial function f. In a later section we will discuss another method for solving (3.1). *Step 3* will be to prove that the function φ that solves (3.1) (normalized so $\|\varphi\|_2 = 1$) generates a multiresolution analysis. This is the trickiest step, because there are simple counterexamples to show that it is not always true (try $a(\gamma)$ equal to 1 for $\gamma = 0, 3$, and otherwise $a(\gamma) = 0$, and $\varphi = \chi_{[0,3]}$, which violates (iv)). Nevertheless, many choices of $a(\gamma)$ do yield a multiresolution analysis. The difficult condition to verify is the orthonormality (iv), and we will have to postpone the discussion of when and why this holds to a later section. In Box 1 we will show how to establish the density (i) and separation (ii), given orthonormality and the additional normalization condition

$$\int\varphi(x)\,dx = 1. \tag{3.9}$$

Now we are ready to move on to *Step 4*, which is the construction of the wavelets themselves.

Proofs of Density and Separation

Lemma B1.1. *Let V_0 be any subspace of $L^2(\mathbb{R})$ which is contained in $L^\infty(\mathbb{R})$ and which has the property that*

$$\|f\|_\infty \leq c\|f\|_2 \quad \text{for all } f \in V_0. \tag{B1.1}$$

Define V_j by the scaling condition (iii) (no assumption of the sort $V_j \subseteq V_{j+1}$ is necessary). Then (ii) holds.

Proof: The scaling condition and a simple change of variable transforms (B1.1) into

$$\|f\|_\infty \leq cm^{j/2}\|f\|_2 \quad \text{for all } f \in V_j. \tag{B1.2}$$

If $f \in \cap V_j$ then (B1.2) holds for all j, and letting $j \to -\infty$ we obtain $\|f\|_\infty = 0$ hence $f = 0$. Q.E.D.

The estimate (B1.1) is easy to obtain in our case. For simplicity assume φ is bounded and has compact support, which will be the case in all our examples. Then by the orthonormality (iv) we have

$$f(x) = \sum_{\gamma \in \mathbb{Z}} \varphi(x-\gamma) \int f(y)\overline{\varphi(y-\gamma)}\,dy = \int K(x,y) f(y)\,dy$$

where $K(x,y) = \Sigma_{\gamma \in \mathbb{Z}} \varphi(x-\gamma)\overline{\varphi(y-\gamma)}$, so

$$|f(x)| \leq \left(\int |K(x,y)|^2\,dy\right)^{1/2} \|f\|_2 = \left(\sum_{\gamma \in \mathbb{Z}} |\varphi(x-\gamma)|^2\right)^{1/2} \|f\|_2$$

and $\Sigma_{\gamma \in \mathbb{Z}} |\varphi(x-\gamma)|^2$ is uniformly bounded (of course much weaker conditions on φ, such as rapid decrease will also imply this).

Lemma B1.2. *Assume φ has compact support and satisfies* (3.1) *and* (3.9), *and the orthonormality condition (iv). Then the density condition (i) holds.*

Sketch of Proof: Let $P_j f(x) = 2^j \Sigma_{\gamma \in \mathbb{Z}} \varphi(2^j x - \gamma) \int f(y)\overline{\varphi(2^j y - \gamma)}\,dy$ denote the orthogonal projection onto V_j. We need to show $\lim_{j \to \infty} P_j f = f$ in L^2 for all $f \in L^2$, which is equivalent to $\lim_{j \to \infty} \|P_j f\|_2^2 = \|f\|_2^2$ by the Pythagorean theorem. It suffices to prove this for $f = \chi_A$, A any interval, by a density argument. But $\|P_j \chi_A\|_2^2 = 2^j \Sigma_{\gamma \in \mathbb{Z}} \int_A \varphi(2^j y - \gamma)\,dy^2 = 2^{-j} \Sigma_{\gamma \in \mathbb{Z}} \left| \int_2^j A \varphi(y-\gamma)\,dy \right|^2$. For large j, $2^j A$ will be a large interval, so essentially either $\int_{2^j A} \varphi(y-\gamma)\,dy = 0$ if $\gamma \notin 2^j A$ or $\int_{2^j A} \varphi(y-\gamma)\,dy = 1$ if $\gamma \in 2^j A$ by (3.9) (for γ in a small neighborhood of the boundary of $2^j A$ this is not quite correct, but in the limit we can ignore this detail). Thus $\|P_j \chi_A\|_2^2 \approx 2^{-j} \#\{\gamma \in 2^j A\} \approx \text{length}(A) = \|\chi_A\|_2^2$ and in the limit this becomes equality. Q.E.D.

Notice that we could essentially reverse the argument to deduce the necessity of the normalization condition (3.9).

§4. THE WAVELETS. We will consider the scaling function φ to be the first element $\varphi = \psi_0$ of a pair of functions ψ_0, ψ_1, with ψ_1 being the wavelet generator. We would like the functions $\{\psi_k(x - \gamma)\}_{\gamma \in \mathbb{Z},\ k=0,1}$ to be an orthonormal basis for V_1. Since the functions $\{\varphi(2x - \gamma)\}_{\gamma \in \mathbb{Z}}$ already form an orthogonal basis for V_1, the functions $\psi_0(x)$ and $\psi_1(x)$ must be linear combinations of $\varphi(2x - \gamma)$, so they must satisfy an identity

$$\psi_k(x) = \sum_{\gamma \in \mathbb{Z}} a_k(\gamma)\varphi(2x - \gamma), \qquad k = 0,1 \tag{4.1}$$

which generalizes (3.1) (of course $a_0(\gamma) = a(\gamma)$). Notice that for $k = 1$ (4.1) is an explicit formula, there is nothing to solve. But what kind of conditions should we put on the coefficients $a_k(\gamma)$? The same reasoning that led to (3.5) leads to

$$\sum_{\gamma \in \mathbb{Z}} a_j(\gamma')\overline{a_k(2\gamma + \gamma')} = 2\delta(j,k)\delta(\gamma,0). \tag{4.2}$$

On the other hand, the condition $\int \varphi(x)\,dx \neq 0$ is not something we can expect to hold for ψ_1 (think of the example of Haar functions), so conditions (3.6) can only be recopied in our new notation

$$\sum_{\gamma \in \mathbb{Z}} a_0(\gamma) = 2. \tag{4.3}$$

Lemma 4.1. *If* $\{\varphi(x - \gamma)\}_{\gamma \in \mathbb{Z}}$ *is an orthonormal set and if* $a_j(\gamma)$ *satisfy* (4.2) *and* (4.3) *then* $\{\psi_k(x - \gamma)\}_{\gamma \in \mathbb{Z},\ k=0,1}$ *is an orthonormal set.*

Proof: It suffices to show

$$\int \psi_j(x)\overline{\psi_k(x - \gamma)}\,dx = \delta(j,k)\delta(\gamma,0). \tag{4.4}$$

Now

$$\int \psi_j(x)\overline{\psi_k(x - \gamma)}\,dx = \sum_{\gamma' \in \mathbb{Z}} \sum_{\gamma'' \in \mathbb{Z}} a_j(\gamma')\overline{a_k(\gamma'')} \int \varphi(2x - \gamma')\overline{\varphi(2x - 2\gamma - \gamma'')}\,dx.$$

But the integral is $(1/2)\delta(\gamma', 2\gamma - \gamma'')$ by the orthonormality of $\varphi(x - y)$ so (4.4) reduces to (4.2). Q.E.D.

Remark. We have omitted the justification of the interchange of series and integrals, but in most of the examples we will look at the series are actually finite sums.

Thus $\{\psi_k(x - \gamma)\}_{\gamma \in \mathbb{Z},\ k=0,1}$ is an orthonormal set of functions in V_1. Is it a basis? (A kind of pseudo dimension counting argument makes this very plausible.) To show that it is a basis it suffices to represent each function $\varphi(2x - \tilde{\gamma})$ as a linear combination, and we know the coefficients will have to be

$$\begin{aligned}\int \varphi(2x - \tilde{\gamma})\overline{\psi_k(x - \gamma)}\,dx &= \sum \overline{a_k(\gamma')} \int \varphi(2x - \tilde{\gamma})\overline{\varphi(2x - 2\gamma - \gamma')}\,dx \\ &= \frac{1}{2}\overline{a_k(\tilde{\gamma} - 2\gamma)}.\end{aligned}$$

Thus we need to show that

$$\frac{1}{2} \sum_{k=0,1} \sum_{\gamma \in \mathbb{Z}} \overline{a_k(\tilde{\gamma} - 2\gamma)} \psi_k(x - \gamma) \tag{4.5}$$

is equal to $\varphi(2x - \tilde{\gamma})$. But if we substitute (4.1) into (4.5) we obtain

$$\sum_{\gamma \in \mathbb{Z}} \left(\frac{1}{2} \sum_{k=0,1} \sum_{\gamma' \in \mathbb{Z}} \overline{a_k(2\gamma' + \tilde{\gamma})} a_k(2\gamma' + \gamma) \right) \varphi(2x - \gamma)$$

so it suffices to show

$$\sum_{k=0,1} \sum_{\gamma' \in \mathbb{Z}} \overline{a_k(2\gamma' + \tilde{\gamma})} a_k(2\gamma' + \gamma) = 2\delta(\gamma, \tilde{\gamma}), \tag{4.6}$$

for $\tilde{\gamma} = 0$ or 1.

Lemma 4.2. (4.6) *always holds, hence* $\{\psi_k(x - \gamma)\}_{\gamma \in \Gamma,\, k=0,1}$ *is an orthonormal basis for* V_1.

Although this is a purely algebraic statement, we postpone the proof until the next section.

Theorem 4.3. *Suppose* φ *generates a multiresolution analysis and* $a_k(\gamma)$ *satisfy* (4.2) *and* (4.3) *with* ψ_k *defined by* (4.1) *and* $\psi_0 = \varphi$. *Then the functions* $\{2^{j/2}\psi_1(2^j x - \gamma)\}$ *for* $j \in \mathbb{Z}$, $\gamma \in \mathbb{Z}$ *form an orthonormal basis of* $L^2(\mathbb{R})$.

Proof: As before, let W_0 denote the orthogonal complement of V_0 in V_1, $V_1 = V_0 \oplus W_0$. We claim $\{\psi_1(x - \gamma)\}_{\gamma \in \mathbb{Z}}$ is an orthonormal basis for W_0. This follows because we have merely taken the basis for V_1 given by Lemma 4.2 and removed $\{\psi_0(x - \gamma)\}_{\gamma \in \mathbb{Z}}$ which is a basis for V_0. By scaling we obtain

$$V_{j+1} = V_j \oplus W_j$$

and

$$\{2^{j/2}\psi_1(2^j x - \gamma)\}_{\gamma \in \mathbb{Z}}$$

is an orthonormal basis for W_j. But

$$L^2(\mathbb{R}) = \bigoplus_{j \in \mathbb{Z}} W_j$$

by the density condition. Q.E.D.

As a simple variation on the theme, which we leave as an exercise to the reader, the set of functions $\{\varphi(x - \gamma)\}$ for $\gamma \in \mathbb{Z}$ together with $\{2^{j/2}\psi_1(2^j x - \gamma)\}$ for $j \geq 0$, $\gamma \in \mathbb{Z}$ form an orthonormal basis of $L^2(\mathbb{R})$. The advantage of this variant is that we scale only to finer and finer resolutions ($j \to +\infty$) and take care of all the coarser resolutions ($j < 0$) by the single family $\{\varphi(x - \gamma)\}_{\gamma \in \mathbb{Z}}$.

In summary, we have reduced the construction of wavelets to the solution of the algebraic identities (4.2) and (4.3), modulo some technical conditions to ensure the

orthonormality condition (iv). *Step 5* will be to actually produce the solutions to (4.2) and (4.3), and *Step 6* will be to establish various properties of the wavelet functions: regularity, decay at infinity, and moment conditions.

The reason we have postponed some of the details in the construction so far is that they require a new technique. So it is now time to open the door and invite Fourier back in.

§5. THE VIEW FROM THE FOURIER TRANSFORM SIDE. Suppose we take the Fourier transform of everything in sight. Because most of our identities have a convolutional structure, we expect a simplification, with multiplicative identities arising in their place. Before doing so, let us return to the orthonormality question, because here the Fourier transform viewpoint gives us an entirely new handle on the problem. Given $\varphi \in L^2$, how can we tell from $\hat{\varphi}$ whether or not $\{\varphi(x-\gamma)\}_{\gamma\in\mathbb{Z}}$ is orthonormal?

It will simplify matters if we adapt the convention (as in **[SW]**) that

$$\hat{\varphi}(x) = \int e^{2\pi i x y}\varphi(y)\,dy \tag{5.1}$$

so that the Fourier inversion formula is just

$$\hat{\hat{\varphi}}(x) = \varphi(-x) \tag{5.2}$$

and the Plancherel formula is

$$\|\varphi\|_2 = \|\hat{\varphi}\|_2 \tag{5.3}$$

(warning: not all the references follow this convention!).

Lemma 5.1. $\{\varphi(x-\gamma)\}_{\gamma\in\mathbb{Z}}$ *is an orthonormal set if and only if*

$$\sum_{\gamma\in\mathbb{Z}} |\hat{\varphi}(\xi+\gamma)|^2 = 1 \quad \textit{for all } \xi. \tag{5.4}$$

Proof: By the Plancherel formula, $\{\varphi(x-\gamma)\}_{\gamma\in\mathbb{Z}}$ is orthonormal if and only if

$$\int e^{2\pi i \xi\gamma}|\hat{\varphi}(\xi)|^2\,d\xi = \delta(\gamma,0). \tag{5.5}$$

But the integral over $\mathbb{R}$ can be broken up into an integral over $[0,1]$ and a sum over $\mathbb{Z}$. Since $e^{2\pi i\xi\gamma}$ is periodic we obtain

$$\int_0^1 e^{2\pi i\xi\gamma} \sum_{\gamma\in\mathbb{Z}} |\hat{\gamma}(\xi+\gamma)|^2\,d\xi = \delta(\gamma,0)$$

which means that the function $\sum_{\gamma\in\mathbb{Z}}|\hat{\varphi}(\xi+\gamma)|^2$ on $[0,1]$ has as Fourier coefficients $\delta(\gamma,0)$, hence must be the constant function given by (5.4). Q.E.D.

Now the scaling identity (4.1) transcribes easily into the condition

$$\hat{\psi}_k(\xi) = A_k(\tfrac{1}{2}\xi)\hat{\varphi}(\tfrac{1}{2}\xi) \tag{5.6}$$

where

$$A_k(\xi) = \frac{1}{2}\sum_{\gamma\in\mathbb{Z}} a_k(\gamma)e^{2\pi i\gamma\xi} \tag{5.7}$$

(exercise, using the definition of the Fourier transform and a change of variable). Notice that $A_k(\xi)$ is smooth and periodic. Then (4.3) says

$$A_0(0) = 1 \tag{5.8}$$

and (3.9) says

$$\hat{\varphi}(0) = 1. \tag{5.9}$$

By iterating (5.6) for $k = 1$ (remember $\psi_0 = \varphi$) we obtain the infinite product representation

$$\hat{\varphi}(\xi) = \prod_{j=1}^{\infty} A_0(2^{-j}\xi) \tag{5.10}$$

(using (5.8) we can justify the local uniform convergence of the infinite product). Substituting (5.10) back into (5.6) we obtain

$$\hat{\psi}_k(\xi) = A_k(\tfrac{1}{2}\xi)\prod_{j=2}^{\infty} A_0(2^{-j}\xi). \tag{5.11}$$

Thus the functions A_k completely and explicitly determine the wavelets.

The most intricate part of the transcription process is the identity (4.2) that the coefficients $a_k(\gamma)$ must satisfy. What does this tell us about the functions A_k? Rather than deal with this question directly (try it as an exercise, after the fact) we repeat the process which led to (4.2)—namely the consistency of (4.1), alias (5.6), with the orthonormality, alias (5.4). In other words, if $\{\varphi(x-\gamma)\}_{\gamma\in\mathbb{Z}}$ is orthonormal then (5.4) must hold, and if (5.6) defines $\hat{\psi}_k$ then we want the analogue of (5.4), namely

$$\sum_{\gamma\in\mathbb{Z}} \hat{\psi}_k(\xi+\gamma)\overline{\hat{\psi}_j(\xi+\gamma)} = \delta_{jk}. \tag{5.12}$$

Now let $\eta_1 = 0$ and $\eta_2 = 1/2$. These are representations of the cosets of the subgroup $\mathbb{Z}$ in $(1/2)\mathbb{Z}$. Then points of the lattice $\mathbb{Z}$ can be represented uniquely as $2(\gamma+\eta_p)$ as γ varies in $\mathbb{Z}$ and $p = 1, 2$. Then

$$\sum_{\gamma\in\mathbb{Z}} \hat{\psi}_k(\xi+\gamma)\overline{\hat{\psi}_j(\xi+\gamma)} = \sum_{p=1}^{2}\sum_{\gamma\in\mathbb{Z}} \hat{\psi}_k(\xi+2(\gamma+\eta_p))\overline{\hat{\psi}_j(\xi+2(\gamma+\eta_p))}$$

by the above parametrization of $\mathbb{Z}$, and if we substitute (5.6) and use the periodicity of A_k we obtain

$$\sum_{p=1}^{2} A_k(\tfrac{1}{2}\xi+\eta_p)\overline{A_j(\tfrac{1}{2}\xi+\eta_p)}\sum_{\gamma\in\mathbb{Z}}\left|\hat{\varphi}(\tfrac{1}{2}\xi+\eta_p+\gamma)\right|^2.$$

The inner sum over $\mathbb{Z}$ yields the constant 1, and so (5.12) yields the consistency condition

$$\sum_{p=1}^{2} A_k(\xi+\eta_p)\overline{A_j(\xi+\eta_p)} = \delta_{jk}. \tag{5.13}$$

This is the Fourier transform equivalent of (4.2). Note that (5.13) implies

$$|A_k(\xi)| \le 1 \tag{5.14}$$

which implies the boundedness of the Fourier transforms $\hat{\psi}_k$.

We can now easily supply the missing proof of Lemma 4.2. Notice that (5.13) says that for every ξ, the 2×2 matrix $\{A_k(\xi + \eta_p)\}$ is unitary by rows. But this is equivalent to being unitary by columns,

$$\sum_{k=0,1} A_k(\xi + \eta_p)\overline{A_k(\xi + \eta_q)} = \delta_{pq}. \tag{B2.1}$$

Now substituting (5.7) into (B2.1) we obtain

$$\sum_{\gamma \in \mathbb{Z}} \left(\frac{1}{4} \sum_{k=0,1} \sum_{\gamma' \in \mathbb{Z}} a_k(\gamma' + \gamma)\overline{a_k(\gamma')} e^{2\pi i \gamma \eta_p} e^{2\pi i \gamma'(\eta_p - \eta_q)} \right) e^{2\pi i \gamma \xi} = \delta_{pq}.$$

Regarding this as an identity between Fourier series expansions we can equate coefficients to conclude

$$\frac{1}{4} \sum_{k=0,1} \sum_{\gamma' \in \mathbb{Z}} a_k(\gamma' + \gamma)\overline{a_k(\gamma')} e^{2\pi i \gamma \eta_p} e^{2\pi i \gamma'(\eta_p - \eta_q)} = \delta_{pq}\delta(\gamma, 0).$$

Choosing $\eta_p = 0$ and summing over q we obtain (4.6) for $\tilde{\gamma} = 0$ since

$$\sum_{q=1}^{2} e^{-2\pi i \gamma' \eta_q} = \begin{cases} 2 & \text{if } \gamma' \in 2\mathbb{Z} \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, choosing $\eta_p = 1/2$, multiplying by $e^{2\pi i \eta_q}$ and summing over q we obtain (4.6) for $\tilde{\gamma} = 1$.

The time has come to grasp the bull by the horns and prove the orthonormality of $\{\varphi(x - \gamma)\}_{\gamma \in \mathbb{Z}}$ directly. For this we will need an additional hypothesis.

Theorem 5.2. *Suppose*

$$A_0(\xi) \neq 0 \quad \text{for } |\xi| \leq \tfrac{1}{4}. \tag{5.15}$$

Then $\{\varphi(x - \gamma)\}_{\gamma \in \mathbb{Z}}$ *is orthonormal.*

Proof: We construct a sequence of functions φ_j such that $\{\varphi_j(x - \gamma)\}_{\gamma \in \mathbb{Z}}$ is orthonormal, and such that $\varphi_j \to \varphi$ in L^2 norm as $j \to \infty$. For φ_0 we simply take $\hat{\varphi}_0(\xi) = \chi_{[-1/2, 1/2]}(\xi)$. Then $\{\varphi_0(\xi - \gamma)\}_{\gamma \in \mathbb{Z}}$ is orthonormal by Lemma 5.1 because (5.4) has exactly one non-zero term.

Inductively define functions φ_j by

$$\hat{\varphi}_j(\xi) = A_0(\tfrac{1}{2}\xi)\hat{\varphi}_{j-1}(\tfrac{1}{2}\xi). \tag{5.16}$$

We claim that $\{\varphi_j(x - \gamma)\}_{\gamma \in \mathbb{Z}}$ is again orthonormal. This follows immediately from (5.13) with $j = k = 0$ and Lemma 5.1. It can also be deduced from

$$\varphi_j(x) = \sum_{\gamma \in \mathbb{Z}} a_0(\gamma)\varphi_{j-1}(2x - \gamma) \tag{5.17}$$

which is the non-Fourier transform version of (5.16), and (4.2). Note that

$$\hat{\varphi}_j(\xi) = \left(\prod_{k=1}^{j} A_0(2^{-k}\xi) \right) \chi_{[-2^{j-1}, 2^{j-1}]}(\xi) \tag{5.18}$$

so that $\hat{\varphi}_j \to \hat{\varphi}$ pointwise, by (5.10).

We would like to show $\varphi_j \to \varphi$ in L^2 norm. This will suffice to complete the proof, because the norm limit of orthonormal sets is an orthonormal set. This is the key point of the proof, where the non-vanishing hypothesis must be used. (As an interesting exercise, see how the argument breaks down for the counterexample given in §3.)

By the Plancherel formula it suffices to show $\hat{\varphi}_j \to \hat{\varphi}$ in L^2 norm, and since we have pointwise convergence we would like to use the dominated convergence theorem. Note first that $\hat{\varphi} \in L^2$ by Fatou's theorem, since it is the pointwise limit of $\hat{\varphi}_j$ and $\|\hat{\varphi}_j\|_2 = 1$. Thus we can use a multiple of $\hat{\varphi}$ as a dominator. By comparing (5.18) and (5.10) we see

$$\hat{\varphi}_j(\xi) = \begin{cases} \dfrac{\hat{\varphi}(\xi)}{\hat{\varphi}(2^{-j}\xi)} & \text{if } |\xi| \le 2^{j-1} \\ 0 & \text{otherwise}. \end{cases} \tag{5.19}$$

We claim that $\hat{\varphi}$ is bounded from below on $[-1/2, 1/2]$. The point is that $\hat{\varphi}$ is continuous, and by (5.15) $A_0(2^{-j}\xi) \neq 0$ for $|\xi| \le 1/2$. Thus $\hat{\varphi}$ doesn't vanish on $[-1/2, 1/2]$, so $|\hat{\varphi}_j(\xi)| \le c|\hat{\varphi}(\xi)|$ for $c = (\inf_{[-1/2,1/2]}|\hat{\varphi}|)^{-1}$. Q.E.D.

§6. THE RECIPE. So now we have indicated all the major steps in the construction, but we have left the first to last. We need to find actual solutions to the algebraic identities (5.8), (5.13) and (5.15). There are several different approaches to this problem. We describe one that is due to Ingrid Daubechies **[D1]**.

We look for solutions with only a finite number of $a_k(\gamma)$ different from zero, which means $A_k(\xi)$ are trigonometric polynomials. This implies that the scaling function φ and wavelet ψ_1 have compact support. This can be seen most easily from the iteration procedure (3.7) and (3.8). Say $a(\gamma) = 0$ unless $\gamma \in [0, N]$; then if f has support in $[0, N]$, so does Sf.

We concentrate first on finding the function A_0, which must satisfy three conditions:

$$A_0(0) = 1 \tag{6.1}$$

$$|A_0(\xi)|^2 + |A_0(\xi + \tfrac{1}{2})|^2 = 1 \tag{6.2}$$

$$A_0(\xi) \neq 0 \quad \text{for} \quad |\xi| \le \tfrac{1}{4} \tag{6.3}$$

(here (6.1) is (5.8), (6.2) is (5.13) for $j = k = 0$ and (6.3) is (5.15)). And, of course, A_0 must be of the form

$$A_0(\xi) = \frac{1}{2} \sum_{\gamma \in \mathbb{Z}} a_0(\gamma) e^{2\pi i \gamma \xi} \quad \text{(finite sum)}. \tag{6.4}$$

Note that $|A_0(\xi)|^2$ is then of the same form.

Now we already know one solution, namely

$$A_0(\xi) = \tfrac{1}{2}(1 + e^{2\pi i \xi}) = e^{\pi i \xi} \cos \pi \xi$$

which yields the Haar wavelets. This was deemed unsatisfactory because the wavelets are not continuous. One way to create continuity and even differentiability is to take convolution powers, or on the Fourier transform side to take ordinary powers. Thus we are tempted to try $A_0(\xi) = (e^{\pi i \xi} \cos \pi \xi)^N$ for some large N. Unfortunately (6.2) no longer holds, but we can fix this up. Note that $\cos \pi(\xi + 1/2) = -\sin \pi \xi$, so that is why $|\cos \pi \xi|^2 + |\cos \pi(\xi + 1/2)|^2 = 1$.

Now take the identity $\cos^2 \pi\xi + \sin^2 \pi\xi = 1$ and raise it to an odd power, say

$$\begin{aligned}1 &= \left(\cos^2 \pi\xi + \sin^2 \pi\xi\right)^5\\ &= \cos^{10} \pi\xi + 5\cos^8 \pi\xi \sin^2 \pi\xi + 10\cos^6 \pi\xi \sin^4 \pi\xi\\ &\quad + 10\cos^4 \pi\xi \sin^6 \pi\xi + 5\cos^2 \pi\xi \sin^8 \pi\xi + \sin^{10} \pi\xi.\end{aligned}$$

Take the first half of the terms for $|A_0|^2$,

$$|A_0(\xi)|^2 = \cos^{10} \pi\xi + 5\cos^8 \pi\xi \sin^2 \pi\xi + 10\cos^6 \pi\xi \sin^4 \pi\xi. \tag{6.5}$$

Replacing ξ by $\xi + 1/2$ turns these into the second half of the terms, so (6.2) is automatic, and (6.1) and (6.3) are easy. This gives a recipe for producing $|A_0|^2$, and it remains to take a square root of the form (6.4). We would also like to take the coefficients $a_0(\gamma)$ in (6.4) to be real, for that will yield a real-valued scaling function (and in the end real-valued wavelets as well). There is a general theorem of F. Riesz that asserts that this is possible, but in this case it is easy enough to accomplish by trial and error. Since

$$\begin{aligned}|A_0(\xi)|^2 &= \cos^6 \pi\xi(\cos^4 \pi\xi + 5\cos^2 \pi\xi \sin^2 \pi\xi + 10\sin^4 \pi\xi)\\ &= \cos^6 \pi\xi\left(\left(\cos^2 \pi\xi - \sqrt{10}\sin^2 \pi\xi\right)^2 + (5 + 2\sqrt{10})\cos^2 \pi\xi \sin^2 \pi\xi\right)\end{aligned}$$

we can take

$$\begin{aligned}A_0(\xi) &= \left(e^{\pi i\xi}\cos \pi\xi\right)^3\left(\cos^2 \pi\xi - \sqrt{10}\sin^2 \pi\xi + i\sqrt{5 + 2\sqrt{10}}\cos \pi\xi \sin \pi\xi\right)\\ &= \frac{1}{8}\left(e^{2\pi i\xi} + 1\right)^3\left(\frac{1 - \sqrt{10}}{2} + \frac{1 + \sqrt{10}}{4}\left(e^{2\pi ix} + e^{-2\pi ix}\right)\right.\\ &\qquad\left. + \frac{1}{4}\sqrt{5 + 2\sqrt{10}}\left(e^{2\pi ix} - e^{-2\pi ix}\right)\right)\end{aligned} \tag{6.6}$$

which is clearly of the form (6.4) with $a_0(\gamma)$ real and $a_0(\gamma) \neq 0$ only if $-1 \le \gamma \le 4$.

To complete the story we need to find $A_1(\xi)$, also of the form (6.4), which satisfies

$$|A_1(\xi)|^2 + \left|A_1(\xi + \tfrac{1}{2})\right|^2 = 1 \tag{6.7}$$

and

$$A_0(\xi)\overline{A_1(\xi)} + A_0(\xi + \tfrac{1}{2})\overline{A_1(\xi + \tfrac{1}{2})} = 0 \tag{6.8}$$

(these are the remaining conditions of (5.13)). Fortunately, this can be accomplished just by taking

$$A_1(\xi) = e^{2\pi i\xi}\overline{A_0(\xi + \tfrac{1}{2})} \tag{6.9}$$

which amounts to setting

$$a_1(\gamma) = (-1)^{\gamma+1}\overline{a_0(1 - \gamma)}. \tag{6.10}$$

Then (6.7) and (6.8) follow directly from (6.2) and the periodicity of A_0. Note also that $a_1(\gamma)$ are real valued if $a_0(\gamma)$ are.

The Fourier transform of ψ_1 is given by (5.11), which now reads

$$\hat{\psi}_1(\xi) = A_1(\tfrac{1}{2}\xi)\prod_{j=2}^{\infty} A_0(2^{-j}\xi) \tag{6.11}$$

with A_0 given by (6.6) and A_1 by (6.9). If we want to obtain the wavelet ψ_1 itself

rather than its Fourier transform we first find $\psi_0 = \varphi$ by iterating the mapping

$$Sf(x) = \sum_{\gamma} a_0(\gamma) f(2x - \gamma) \tag{6.12}$$

starting with any reasonable f satisfying $\int f(x)\,dx = 1$, and then setting

$$\psi_1(x) = \sum_{\gamma} a_1(\gamma) \varphi(2x - \gamma). \tag{6.13}$$

See FIGURES 2 and 3.

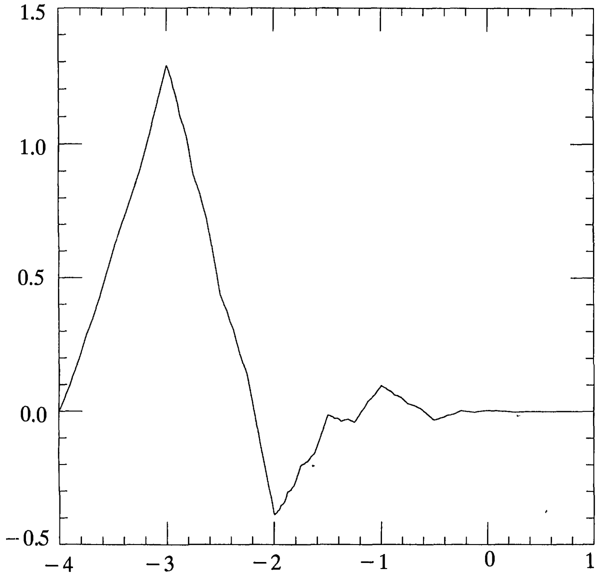


Figure 2. The graph of the scaling function φ, courtesy of David Aronstein.

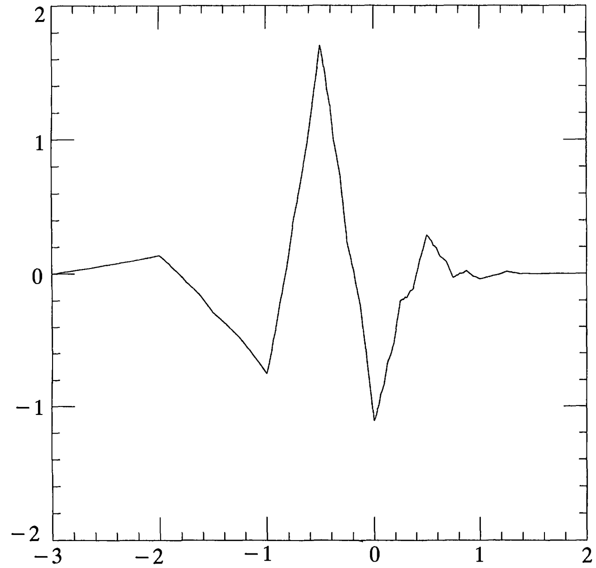


Figure 3. The graph of the wavelet generator ψ_1, courtesy of David Aronstein.

There is an alternative approach to constructing the scaling function that yields a different wavelet basis. It has the advantage of requiring less algebra, but the disadvantage of producing wavelets that are not compactly supported. Start with the Haar basis scaling function $\chi_{[0,1]}$, whose Fourier transform is $e^{\pi i \xi}(\sin \pi\xi / \pi\xi)$, and take the N-fold convolution product

$$g = \chi_{[0,1]} * \chi_{[0,1]} * \cdots * \chi_{[0,1]} \qquad (N \text{ factors})$$

so that

$$\hat{g}(\xi) = \left(e^{\pi i \xi} \frac{\sin \pi\xi}{\pi\xi} \right)^N.$$

It is easy to see that $g \in C^{N-1}$, but of course we have destroyed the orthonormality of translates by $\mathbb{Z}$ that $\chi_{[0,1]}$ had. Too bad, but this is easily fixed. Write

$$h(\xi) = \left(\sum_{k \in \mathbb{Z}} |\hat{g}(\xi + k)|^2 \right)^{1/2}$$

and observe that h is periodic and

$$0 < c_1 \leq h(\xi) \leq c_2 < \infty.$$

Then we have only to take

$$\hat{\varphi}(\xi) = \hat{g}(\xi)/h(\xi)$$

and (5.4) is automatic, so we have the orthonormality of $\{\varphi(x - \gamma)\}_{\gamma \in \mathbb{Z}}$. Notice that $\hat{g}(0) = 1$ and $\hat{g}(\gamma) = 0$ for $\gamma \neq 0$ so $\hat{\varphi}(0) = 1$ as required. And it is not difficult to show that $\varphi \in C^{N-1}$.

What about the scaling identity? Well, it certainly holds for g, namely

$$\hat{g}(\xi) = B(\xi/2)\hat{g}(\xi/2)$$

where

$$B(\xi) = (e^{\pi i \xi} \cos \pi\xi)^N$$

has the required form (6.4). It then follows that

$$\hat{\varphi}(\xi) = A_0(\xi/2)\hat{\varphi}(\xi/2)$$

where

$$A_0(\xi) = B(\xi)h(\xi)/h(2\xi).$$

Now A_0 is periodic, so it must have the form (6.4), but the sum is no longer finite. This is where we lose the compact support of φ. On the other hand A_0 is clearly smooth, so the Fourier coefficients in (6.4) must be rapidly decreasing, which implies that φ is rapidly decreasing.

The construction of $A_1(\xi)$ and the wavelet Fourier transform $\hat{\psi}_1(\xi)$ then proceeds via (6.9) and (6.11) as before.

§7. SMOOTHNESS OF WAVELETS. How smooth are our wavelets? Since we understand them best on the Fourier transform side, we will use the principle that decay at infinity of $\hat{\varphi}$ implies smoothness of φ (we will establish smoothness of the scaling function and pass it on to the wavelets via (6.13)). For example, it is easy to show

$$|\hat{\varphi}(\xi)| \leq c(1+|\xi|)^{-N-1-\varepsilon} \tag{7.1}$$

implies $\varphi \in C^N$. So how do we establish (7.1)?

We have the infinite product representation (5.10) which says

$$\hat{\varphi}(\xi) = \prod_{k=1}^{\infty} A_0(2^{-k}\xi) \tag{7.2}$$

and A_0 is periodic. Since each factor does not decay at infinity, why should the product? This is a mystery, which is best solved by looking at the simplest case, $A_0(\xi) = \cos \pi\xi$. Then

$$\prod_{k=1}^{\infty} \cos 2^{-k}\pi\xi = \frac{\sin \pi\xi}{\pi\xi} \tag{7.3}$$

does decay at the rate $O(|\xi|^{-1})$. (Formula (7.3) was proved by Euler, but special cases were known by Francois Viète in the late 1500's. You can prove it by considering the Fourier transform of $\chi_{[-1/2,1/2]}$ and its scaling properties.)

Clearly, for most choices of ξ, the values of $\cos 2^{-k}\pi\xi$ will occasionally become small, and that makes the product (7.3) small. You might try to get around this by taking $\xi = 2^N$ for large N. Thus $\cos 2^{-k}\pi\xi = \pm 1$ for $k = 1, \ldots, N$, so there is no decay, but then $\cos 2^{-N-1}\pi\xi = 0$ wipes you out. You can try to quantify this line of reasoning, but there is no great payoff in showing, for example, that $\sin \pi\xi/\pi\xi = O(|\xi|^{-2/3})$, so we will take (7.3) as our starting point.

The expression (6.6) for A_0, or any of its more complicated cousins, contains $\cos\pi\xi$ as a factor, many times. Thus $\hat{\varphi}(\xi)$ contains $\sin \pi\xi/\xi$ as a factor many times, hence we expect decay. Unfortunately, the other factor grows. It is easier to work with $|A_0|^2$ given by (6.5), if we remember to take the square root at the end. We have, for the special case considered,

$$|A_0(\xi)|^2 = (\cos \pi\xi)^6(\cos^4 \pi\xi + 5\cos^2 \pi\xi \sin^2 \pi\xi + 10\sin^4 \pi\xi).$$

The first factor produces decay $O(|\xi|^{-6})$. The second factor can be written $1 + 3\sin^2 \pi\xi + 6\sin^4 \pi\xi$ so it clearly has a maximum value 10 at $\xi = 1/2$. We can obtain a crude estimate for the growth rate produced by the second factor by the following reasoning: if $|\xi| \approx 2^N$ then there will be about N factors where $2^{-k}|\xi|$ is large, so an upper bound for the product is a constant times 10^N. But $10^N \approx |\xi|^\alpha$ for $\alpha = \log 10/\log 2 \approx 3.32$. So the growth rate is at most $O(|\xi|^{3.32})$ so the combination gives $O(|\xi|^{-2.68})$ for $|\hat{\varphi}(\xi)|^2$ hence $O(|\xi|^{-1.34})$ for $\hat{\varphi}(\xi)$.

This is a disappointing estimate. According to (7.1) it suffices only to show that φ is continuous. It can be improved, but not by a lot. To see why, consider $\xi = 2^N/3$. Then for each of the N factors $2^{-k}\xi = 2^{N-k}/3$, $1 \leq k \leq N$, we have $1 + 3\sin^2 2^{N-k}\pi/3 + 6\sin^4 2^{N-k}\pi/3 = 1 + 3\cdot(\sqrt{3}/2)^2 + 6(\sqrt{3}/2)^4 = 6.625$ so a lower bound for α is $\log 6.625/\log 2$ which yields $O(|\xi|^{-1.636})$ as the optimal improvement.

If we consider the family of wavelets constructed as outlined in §6, we will have $|A_0(\xi)|^2$ written as the product of higher and higher powers of $\cos \pi\xi$ by more and more complicated second factors. Thus we have faster decay times faster growth in $\hat{\varphi}(\xi)$. Which wins? Well, it is a close race! It turns out that the decay wins, but the

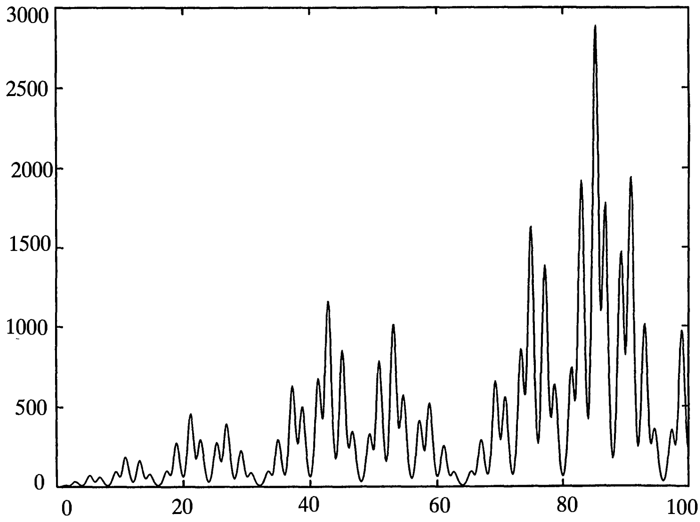


Figure 4. The graph of $\hat{\varphi}$, after factoring out a power of $\sin \pi x / \pi x$, courtesy of Prem Janardhan and David Rosenblum.

crude method of estimating the growth used above is not good enough to show this. The final result ([**D1**], [**C2**]) is that to create wavelets of class C^N we need to carry out the construction starting with $(\cos^2 \pi\xi + \sin^2 \pi\xi)^M = 1$ for M on the order of $5(N+1)$. This means that there is a rather high price to pay in terms of complexity (the algebra required to pass from $|A_0|^2$ to A_0, for example) in order to gain a moderate amount of smoothness. (More recently, better techniques have been found to estimate the smoothness directly, without involving the Fourier transform [**DL**].) FIGURE 4 shows the graph of $\hat{\varphi}(\xi)$. See [**JRS**] for a discussion of the surprising self-similarity properties of this function.

In addition to smoothness, another important property of wavelets is the vanishing moment conditions

$$\int_{-\infty}^{\infty} x^k \psi_1(x)\, dx = 0, \quad k = 0, 1, \dots, N \tag{7.4}$$

which are equivalent to the vanishing of the Fourier transform to high order at the origin,

$$\left(\tfrac{d}{d\xi}\right)^k \hat{\psi}_1(0) = 0, \quad k = 0, 1, \dots, N. \tag{7.5}$$

In contrast to smoothness, however, it is only the wavelet, not the scaling function, which enjoys this property. The significance of this condition is that it implies a weak form of localization in the frequency (Fourier transform) variable, since the Fourier transform of $\psi_1(2^j x - k)$ is mainly concentrated around values of $|\xi|$ on the order of 2^j. (There is yet another family of wavelets in which the Fourier transform is actually supported in an annular region $c_1 2^j \le |\xi| \le c_2 2^j$. See [**M**] for a description of these "Littlewood-Paley" type wavelets.) For our wavelets the verification of (7.5) is easy. From (6.11) we see that $\hat{\psi}_1$ has a factor $A_1((1/2)\xi)$, and from (6.9) we see that A_1 at $\xi = 0$ has the same order zero as A_0 at $\xi = 1/2$. But A_0 has a factor of $\cos \pi\xi$ to a power, hence vanishes at $\xi = 1/2$ to order 3 in our particular example, and to order M if we start with $(\cos^2 \pi x + \sin^2 \pi x)^M = 1$ in our construction. Note that in general conditions (6.1) and (6.2) imply that

$A_0(1/2) = 0$, and the flatter we make A_0 near $\xi = 0$, the more it vanishes near $\xi = 1/2$.

§8. CONCLUDING REMARKS. Why not try to create your own designer wavelets by programming the recipe given in §6, and taking the square root of $|A_0(\xi)|^2$ in a different way? For a more detailed discussion of the Riesz Lemma for doing this see **[D1]**.

For further information about wavelets, including historic accounts and attribution of results, see the books **[M]**, **[BF]**, **[BC]** or the expository lectures **[D2]** and **[FJW]**. The term "wavelet" is also used to describe expansions in terms of functions which are not orthogonal. These wavelets have a simpler algebraic description, which is useful for some applications. An expanded version of this article, including a discussion of wavelet bases in several variables, will appear in **[BF]**. None of the theorems or proofs presented here are original; I have only tried to organize the material in a way that is easy to digest.

REFERENCES

[BF] J. Benedetto and M. Frazier (editors), "Wavelets: Mathematics and Applications," CRC Press, to appear.

[BC] G. Beylkin, R. Coifman, I. Daubechies, S. Mallet, Y. Mayer, M. B. Ruskai and L. Raphael (editors), *Wavelets and Their Applications*, Jones and Bartlett, 1992.

[C1] A. Cohen, *Ondelettes, analyses multi-résolutions et filtres miroir en quadrature*, Annales de l'Institut Henri Poincaré, Analyse non linéaires 7 (1990), 439–459.

[C2] A. Cohen, *Construction de bases d'ondelettes α-Hölderiennes*, Rev. Mat. Iberoamericana 6 (1990), 91–108.

[D1] I. Daubechies, *Orthonormal bases of compactly supported wavelets*, Comm. Pure Appl. Math. 41 (1988), 909–996.

[D2] I. Daubechies, *Ten Lectures on Wavelets*, Notes for the CBMS Conference (Lowell), SIAM 1992.

[DL] I. Daubechies and J. Lagarias, *Two-scale difference equations, I and II*, SIAM J. Math. Anal. 22 (1991), 1388–1410, 23 (1992), 1031–1079.

[FJW] M. Frazier, B. Jawerth and G. Weiss, *Littlewood-Paley theory and the study of functions spaces*, CBMS, Regional Conference Series in Mathematics, no. 79, American Mathematical Society, Providence, RI, 1991.

[JRS] P. Janardhan, D. Rosenblum and R. S. Strichartz, *Numerical experiments in Fourier asymptotics of Cantor measures and wavelets*, to appear, *Exper. Math.*.

[M] Y. Meyer, *Ondelettes et Operateurs*, 2 volumes, Hermann, Paris, 1990.

[SW] E. M. Stein and G. Weiss, *Introduction to Fourier Analysis on Euclidean Spaces*, Princeton University Press, 1971.

Mathematics Department
Cornell University
Ithaca, NY, 14853

A Matrix Maximum

William C. Waterhouse

1. INTRODUCTION. In a recent paper [**KZ**], Kwong and Zettl described the solution to a maximization problem involving a 2 by 2 matrix A with real entries. They used a special way of normalizing the matrix, and it led them into computations that could only be done as symbolic manipulations on a computer. I want to show how a more geometric normalization will uncover a latent symmetry in the problem and thereby reduce the computation to comprehensible steps.

To understand the normalization, we should begin with a simpler, more familiar question: what is the maximum of $\|Ax\|/\|x\|$, where $\|x\|$ denotes length in the plane? The first thing to observe is that scaling x does not change the ratio, and thus we only have to consider its values for x on the unit circle. Now A clearly must map the unit circle $x_1^2 + x_2^2 = 1$ to an ellipse (or straight line segment, if A is singular). Thus if the semi-axes of the ellipse are (say) k and m, then the larger of those two is the maximum of $\|Ax\|/\|x\|$.

We could turn this geometric analysis into a computation of the maximum, but it is more important to see how it leads to an expression for the structure of A (see Figure 1). Let $R(\phi)$ be the matrix of rotation by angle ϕ, so

$$R(\phi) = \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix}.$$

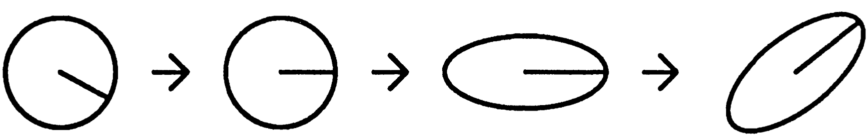


Figure 1. Structure of a Linear Mapping

The inverse of $R(\phi)$ is of course $R(-\phi)$. Take one of the half-axes of the ellipse, say of length k, and suppose it makes an angle α with the positive x-axis. Then $R(-\alpha)A$ maps the unit circle to an ellipse with axes along the coordinate axes. The half-axis lengths are still k and m, and so we can multiply by a diagonal matrix to get $\operatorname{diag}(k, m)^{-1}R(-\alpha)A$ mapping the unit circle to itself. Hence it is an orthogonal mapping, either some rotation $R(\beta)$ or $\operatorname{diag}(1, -1)$ times $R(\beta)$. Multiplying through and absorbing any negative sign into m, we obtain the following result, a variant of the "singular value decomposition."

Theorem 0. *Every 2 by 2 matrix A can be written in the form*

$$A = R(\alpha)\begin{pmatrix} k & 0 \\ 0 & m \end{pmatrix}R(\beta)$$

for some angles α, β and some constants k, m.

You can verify that this geometric proof [**OG**, p. 343–6] does indeed have a modification that works when A is singular. The same idea can be stated purely in terms of linear algebra: the first step is to observe that AA^{tr} is symmetric with positive eigenvalues, and hence it equals $R(\alpha)\text{diag}(k^2, m^2)R(-\alpha)$ for suitable k, m, α. Then if you take $B = R(\alpha)\text{diag}(k, m)R(-\alpha)$, you can easily verify that $B^{-1}A$ is orthogonal. (The theorem is actually valid in any number of variables, with special orthogonal matrices in place of rotations. See [**H**, p. 169] or [**G**, p. 286].) For our purposes, the advantage of this decomposition of A is that it incorporates information about the relation between $\|Ax\|$ and $\|x\|$. Observe that we have our choice of the order in which the diagonal entries occur, and so for nonzero A we can always suppose that k is nonzero.

2. NORMALIZING THE PROBLEM. Fix now an invertible A. The problem solved by Kwong and Zettl is to find the maximum of

$$\frac{\|Ax\|^2}{\|x\| \cdot \|A^2x\|}$$

for nonzero x. As A is invertible, we can make a change of variable to replace x by Ax; thus it is equivalent to say that we want the maximum of

$$\frac{\|x\|^2}{\|A^{-1}x\| \cdot \|Ax\|}.$$

Clearly the ratio is again homogeneous in x, so the maximum can be found on the unit circle. As Kwong and Zettl observed, we have

$$\|Ax\| = \|R(\phi)Ax\| = \|R(\phi)AR(-\phi)[R(\phi)x]\|,$$

and similarly for A^2, so the maximum for A is the same as for $R(\phi)AR(-\phi)$. Furthermore, in this problem there is a homogeneity in A, so the maximum does not change if we multiply A by a nonzero scalar. Now the decomposition of the previous section shows us a nice way to simplify A using these operations: we can first conjugate by a rotation to cancel the factor $R(\alpha)$, and then we can multiply by a scalar to make the first entry in the diagonal factor equal to 1. Thus we have a promising normalization:

Theorem 1. *Let A be any 2 by 2 matrix not identically zero. Multiplying by a scalar and conjugating by a rotation, we can reduce A to the form $MR(\theta)$, where θ is some angle and $M =$ diag$(1, m)$ for some constant m.* □

We now take A to be of the form $MR(\theta)$, and we let $K(m, \theta)$ be the maximum as x varies over the unit circle. To eliminate square roots, we can work with the square of the ratio and compute $K^2(m, \theta)$. Let t parametrize the unit circle by angle, so $x(t)$ will have entries $\cos(t)$ and $\sin(t)$. For brevity, set

$$Q(t) = \|Mx(t)\|^2 = \cos^2(t) + m^2\sin^2(t) = m^2 + (1 - m^2)\cos^2(t). \quad (1)$$

Obviously $R(\theta)x(t) = x(t + \theta)$, so

$$\|Ax(t)\|^2 = \|MR(\theta)x(t)\|^2 = Q(t + \theta).$$

Similarly, we have

$$\|A^{-1}x(t)\|^2 = \|R(-\theta)M^{-1}x(t)\|^2 = \|M^{-1}x(t)\|^2 = Q(\pi/2 - t)/m^2.$$

Thus we have:

Lemma 2. *Let* $f(t) = m^2/Q(t + \theta)Q(\pi/2 - t)$. *Then* $K^2(m, \theta) = \max_t f(t)$. □

Before going on, it might be good to look at the graph of $f(t)$ in a few examples. The two basic types are illustrated in Figures 2 and 3. All use the same angle $\theta = \pi/4$, so they also illustrate the change of behavior with m. Observe that there are certain values of t depending only on θ (in this case, $t = \pi/8$ and $t = \pi/2 +$

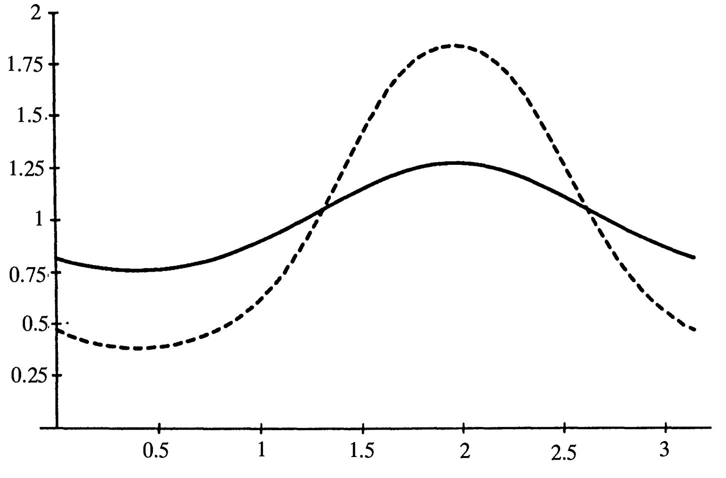


Figure 2. $f(t)$ with $\theta = \pi/4$ and $m = 1.2$ (solid), $m = 1.8$ (dashed)

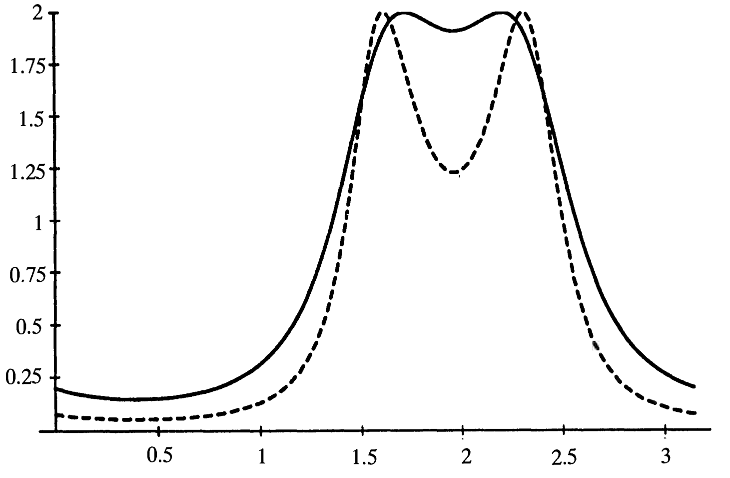


Figure 3. $f(t)$ with $\theta = \pi/4$ and $m = 3$ (solid), $m = 5$ (dashed)

$\pi/8$) that always give local extrema. For large m, however, the absolute maximum occurs elsewhere and has a value independent of m. We shall show that these properties are true in general.

3. THE LATENT SYMMETRY. It is clear from the original homogeneity that $f(t+\pi) = f(t)$. But the expression for f in terms of Q shows that there is also a latent symmetry. To bring it out, we set $p = (\pi/2 + \theta)/2$ and $u = t - (\pi/2 - \theta)/2$; then we get $f(t) = m^2/g(u)$ with

$$g(u) = Q(p+u)Q(p-u). \tag{2}$$

When we expand, we get

$$\begin{aligned} Q(p+u) &= m^2 + (1-m^2)[\cos(p)\cos(u) - \sin(p)\sin(u)]^2 \\ &= m^2 + (1-m^2)\left[\cos^2(p)\cos^2(u) + (1-\cos^2(p))(1-\cos^2(u))\right] \\ &\quad - 2(1-m^2)\cos(p)\cos(u)\sin(p)\sin(u). \end{aligned} \tag{3}$$

The symmetry now lets us observe that $Q(p-u)$ is the same as $Q(p+u)$ except for the sign of the last term, which will be reversed. Thus the product $g(u)$ will be the difference of the squares. We can see at once that sines and cosines will occur in g only as squares, and thus we are going to be able to use cosines alone; furthermore, we see that the result will be quadratic in the variable $W = \cos^2(u)$. To find it explicitly, we have to do some straightforward computation. Of course you can save time and avoid mistakes by doing it on a computer, but it can certainly be handled by hand. Here is the result.

Lemma 3. *Set $W = \cos^2(u)$. Then $g(u) = G(W)$ where*

$$\begin{aligned} G(W) = (1-m^2)^2 W^2 &+ 2(1-m^2)\left[m^2\cos^2(p) + \cos^2(p) - 1\right]W \\ &+ (1-m^2)^2\cos^4(p) - 2(1-m^2)\cos^2(p) + 1. \quad \square \end{aligned}$$

4. COMPUTATION OF THE CRITICAL VALUES. Our $G(W)$ is identically 1 if $m^2 = 1$; otherwise it is quadratic. The square term is positive, and hence the unique extreme value of G will be its absolute minimum. There is basically no difficulty in finding its extremum; again the computation takes a little work, but it is not hard. The appearance of the factor $(1-m^2)$ to appropriate powers in the coefficients helps make the result particularly nice:

Lemma 4. *For $m^2 \neq 1$, the function $G(W)$ has a unique extremum (a minimum) at the point*

$$W = \frac{1 - \cos^2(p) - m^2\cos^2(p)}{1-m^2}. \tag{4}$$

The value at that point is $4m^2\cos^2(p)(1-\cos^2(p))$. $\square$

Now we can begin to translate this result back into our original variables. We had $g(u) = G(\cos^2(u))$, and hence we have

$$g'(u) = -2\cos(u)\sin(u)G'(\cos^2(u)).$$

Thus the critical points of $g(u)$ occur at points where $\cos^2(u)$ is either 0 or 1 or the W in (4) where G has its minimum. When $\cos^2(u)$ is either 0 or 1, we can see that the last term in (3) is zero, and so we can evaluate $g(u) = Q(p+u)Q(p-u)$

directly; we get the values

$$\left[m^2 + (1 - m^2)\cos^2(p)\right]^2 \quad \text{and} \quad \left[m^2 + (1 - m^2)\sin^2(p)\right]^2.$$

We have $p = (\pi/2 + \theta)/2$, and hence

$$2\cos^2(p) - 1 = \cos(2p) = \cos(\pi/2 + \theta) = -\sin(\theta).$$

Thus $\cos^2(p) = (1 - \sin(\theta))/2$, and similarly $\sin^2(p) = (1 + \sin(\theta))/2$. The values at the first two types of critical points then come out to be

$$\left(\frac{m^2 + 1 \pm (1 - m^2)\sin(\theta)}{2}\right)^2. \tag{5}$$

The value at the minimum of G is even simpler; it comes out to be just $m^2\cos^2(\theta)$.

Of course it is possible that the G-minimum occurs at a point that cannot be a value of $\cos^2(u)$. The reduction from p to θ shows that this minimum occurs when

$$W = \frac{1 - m^2 + (1 + m^2)\sin(\theta)}{2(1 - m^2)}.$$

Hence we need to determine when this value is between 0 and 1. That is just a two-line computation, yielding the condition

$$\left|\left(\frac{1 + m^2}{1 - m^2}\right)\sin(\theta)\right| \leq 1. \tag{6}$$

Thus we have finished our computations, which we can summarize quite briefly:

Theorem 5. *The function $g(u)$ has the values* (5) *at the critical points where u is a multiple of $\pi/2$. If* (6) *is false, these are the only critical points; but if* (6) *is true, g also has an absolute minimum with value $m^2\cos^2(\theta)$.* □

5. THE MAIN THEOREM. If we multiply by the denominator, we can state the basic inequality in a way that makes sense for singular matrices, and (like **[KZ]**) we include that in our final version of the result.

Theorem 6. *Let A be a nonzero* 2 *by* 2 *matrix, and let scaling and conjugation by rotations reduce A to the form $MR(\theta)$, where $M = \operatorname{diag}(1, m)$. Let K denote the smallest constant (if any) that makes $\|Ax\|^2 \leq K \cdot \|x\| \cdot \|A^2x\|$ true for every vector x. If*

$$\left|\left(\frac{1 + m^2}{1 - m^2}\right)\sin(\theta)\right| \leq 1,$$

then $K = 1/|\cos(\theta)|$. When $m = 0$ and $\cos(\theta) = 0$, the inequality does not hold with any constant. In all other cases, K is the larger of the two values

$$\frac{2|m|}{m^2 + 1 \pm (1 - m^2)\sin(\theta)}.$$

Proof: When $m \neq 0$, this theorem follows at once from (2), Lemma 2, and Theorem 5. (The case $m^2 = 1$ was excluded in Section 4, but the theorem gives the correct answer in that case, as (6) is then not true.) For $m = 0$, we can hold θ fixed and let m approach 0; as we are working with the compact set of vectors of norm 1, the constant K in the limiting case will be the limit of the approximating ones. If

$\sin(\theta) \neq \pm 1$, then the expression in (6) is less than 1 for all m close to 0; the extreme is thus equal to $1/|\cos(\theta)|$, as the theorem says. If $\sin(\theta) = \pm 1$, then we are in the last case for all small m; the maximum there is $1/|m|$, which goes to infinity as m goes to 0. $\square$

The case where no bound exists corresponds to the nilpotent normalized matrix

$$\begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}.$$

In the other cases, we know the u giving the maximum, and so we could trace back the normalizations to compute the angle of maximum for the original A.

6. RELATION TO THE EARLIER TREATMENT. In **[KZ]**, the matrices were normalized to have their diagonal entries both equal to 1 or both equal to 0. Consequently, the results there look rather different, and I want to conclude by displaying the connection with the formulas derived here. First we rotate: if we set $\psi = (\pi/2 - \theta)/2$, then it is easy to check that

$$R(-\psi)MR(\theta)R(\psi) = \frac{m+1}{2} \begin{pmatrix} \cos(\theta) & \dfrac{m-1}{m+1} - \sin(\theta) \\ \dfrac{m-1}{m+1} + \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

To avoid special cases and sign distinctions, let us suppose that $m > 1$ and both $\sin(\theta)$ and $\cos(\theta)$ are positive. We can then scale to get

$$\begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}$$

with

$$b = \frac{1}{\cos(\theta)} \left(\frac{m-1}{m+1} - \sin(\theta) \right) \quad \text{and} \quad c = \frac{1}{\cos(\theta)} \left(\frac{m-1}{m+1} + \sin(\theta) \right).$$

Using the notation of **[KZ]**, we introduce $h = c - b$ and $r = (1 + h^2/4)^{1/2}$. Their assertion is that K for this matrix is $|1 - bc|/(1 + b^2)$ except when b is between $2(1 - r)/h$ and $2(1 + r)/h$, in which case $K = r$. It is easy to check that (in our notation) $h = 2\tan(\theta)$ and $r = 1/\cos(\theta)$, while $|1 - bc|/(1 + b^2)$ comes out to be

$$\frac{2m}{m^2 + 1 + (1 - m^2)\sin(\theta)}.$$

Readers might find it a pleasant exercise to check that the betweenness condition on b is equivalent to our condition (6).

REFERENCES

[G] F. R. Gantmacher, *The Theory of Matrices*, trans. K. A. Hirsch, Vol. I, Chelsea, 1959.

[H] P. R. Halmos, *Finite-Dimensional Vector Spaces*, Van Nostrand, 1958.

[KZ] M. K. Kwong and A. Zettl, Norm inequalities for the powers of a matrix, *Amer. Math. Monthly*, 98 (1991), 533–538.

[OG] W. F. Osgood and W. C. Graustein, *Plane and Solid Analytic Geometry*, Macmillan, 1920.

Department of Mathematics
The Pennsylvania State University
University Park, PA 16802

Chaotic Motion of a Pendulum with Oscillatory Forcing

S. P. Hastings and J. B. McLeod

I. INTRODUCTION. The mathematical theory of "chaos" has grown rapidly in the last twenty years, with one landmark being the 1975 paper [**9**] of Y. Li and J. Yorke which appeared in this journal. Indeed, we understand that this paper included the first use of the word chaos in the context of dynamical systems. The subject dominates dynamical systems theory today, in the literature of both mathematics and physics. This is despite a lack of unanimity on what sorts of behavior should be called chaotic, or any firm definition of associated concepts, such as "strange attractor," or "sensitivity to initial conditions."

The Li-Yorke paper, which turned out to be a rediscovery of some of the results of the Soviet mathematician A. N. Sharkovsky eleven years earlier [**3**, **13**], dealt with iterations of maps of an interval into itself. Even today, chaos theory is far more developed in the case of maps, in one or two dimensions particularly, than it is for smooth dynamical systems, such as differential equations. This is largely because differential equations are so much harder. For example, the famous set of differential equations found by E. N. Lorenz [**10**] in the context of meteorological investigations is still not understood very well, since there are no proofs of chaotic behavior.

There is, nevertheless, considerable theory for the case of ordinary differential equations (much less for partial equations) and several monographs are available expounding this theory. One of the best known is the book [**6**] by J. Guckenheimer and P. Holmes. There we learn again that the Soviets were ahead, since there is extensive discussion of the theories of V. K. Melnikov, from 1963 [**11**], and L. P. Shil'nikov, from 1968 [**14**]. The techniques of both of these pioneers were designed to reduce the study of certain systems of differential equations to the study of finite-dimensional maps. They show that imbedded in the phase space for these systems one can find a "horseshoe" map, which is a creation of S. Smale in the 1960s [**15**], and which enables one to show, for example, that the system in question has infinitely many periodic solutions. Not all workers accept this as a criterion for chaos, but it is the focus of much work, and in most cases, all that has been proved for smooth systems of differential equations.

The book by Guckenheimer and Holmes, like other literature in this field, is not easy reading. The theory was, and remains, incomplete and this is reflected in the unfinished nature of many of the results. For example, the following remark from their discussion of the concept of strange attractor is probably still valid.

> "In trying to piece together a coherent picture of this situation, we enter a realm in which the theory remains in an unsatisfactory state. There are paradoxes in which different theorems appear to be steering us toward opposite conclusions."...

We do not propose to resolve such problems here, or even to give an exposition of these fascinating concepts. Rather, we concentrate on the intuitive idea that a differential equation exhibits chaos if it has many solutions which are bounded and which are erratic and unpredictable in some sense. Within this limited scope there are a number of rigorous results, for smooth differential equations as well as for maps.

Generally these have been obtained by methods, like those of Melnikov and Shil'nikov, which in some way reduce the study of the differential equation to the study of a related map in a lower dimensional space. For example, if we are studying an autonomous system of three first-order ordinary differential equations, the related map is two-dimensional, taking some subset of the plane into itself. The goal of this paper is to show that results of this sort are accessible by different, and we think simpler, methods, which involve study of solutions of the differential equation directly rather than through a related map. We do this for a particular example, the equation for a pendulum with oscillating support, for illustration. The same technique can be applied to other equations, and some examples are given in [7] and [**8**].

II. EQUATION OF MOTION FOR A PENDULUM. First consider a simple pendulum, consisting of a mass m at the end of a massless rod of length l, which pivots on a frictionless support that forces the pendulum to move in a vertical plane (FIGURE 1).

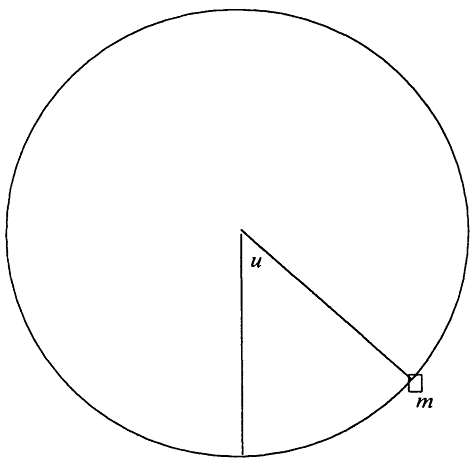


Figure 1. We consider a pendulum free to rotate in a full circle.

At time τ the rod makes an angle $u(\tau)$ with the vertical. The forces to be considered are the gravitational force mg and the damping due to air resistance as the pendulum swings. This is assumed to be proportional to the angular velocity $(du/d\tau) = \dot{u}(\tau)$. Applying Newton's law of motion, we obtain the ordinary differential equation

$$ml\ddot{u} + c\dot{u} + mg \sin u = 0,$$

where c is the positive constant of proportionality. We immediately rescale to get the dimensionless version, by setting $t = \sqrt{g/l}\,\tau$ and $y(t) = u(\tau)$. Letting

$(dy/dt) = y'$, we get

$$y'' + ky' + \sin y = 0, \tag{1}$$

where $k = c/m\sqrt{gl}$.

The phase plane obtained by plotting $y'(t)$ against $y(t)$ is well known, and can be found in many introductory texts on ordinary differential equations, such as [**2**]. In Figure 2 we show the cases $k = 0$ and $0 < k < 2$.

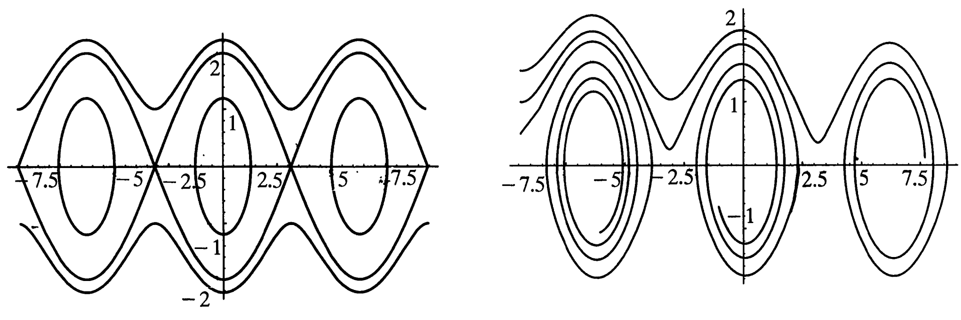


Figure 2. Two phase planes for the pendulum, one undamped, the other damped.

When $k = 0$ (no damping) the equation is called "conservative," because there is a function of the solution which is conserved, or, in other words, is constant as t varies. This is the so-called "energy" function associated with the pendulum. If $(y(\cdot), y'(\cdot))$ is a solution, the associated energy is

$$E(t) = \frac{y'(t)^2}{2} - \cos y(t),$$

and is the usual energy function from physics, being a sum of the kinetic energy $y'(t)^2/2$ and a potential energy term $-\cos y(t)$, which is at a minimum when the pendulum is at its stable rest point, $y = 0$. To see that E is constant in the absence of damping, differentiate the expression for E and use (1) with $k = 0$.

Figure 2 illustrates conservation of energy when $k = 0$ because there is a family of orbits which are closed smooth curves, and represent periodic solutions. These are solutions with low energy. On the other hand, if the initial velocity is large, so that $E(t)$ is large, then the trajectory in phase space is unbounded, and represents a pendulum which continues to rotate in the same direction, making repeated complete rotations without loss of energy. It is important to observe that there are intermediate trajectories, such as the one which tends to the point $(-\pi, 0)$ in phase space as $t \to -\infty$, and to $(\pi, 0)$ as $t \to \infty$.

A trajectory in the phase plane of an autonomous differential equation represents many solutions, which can be characterized as passing through the same point in phase space but at different times. Corresponding to the trajectory connecting $(-\pi, 0)$ to $(\pi, 0)$ as t increases, which exists when $k = 0$, there is a unique solution y_0 of (1) such that

$$y_0(0) = 0, \qquad \lim_{t \to \infty} y_0(t) = \pi, \qquad \lim_{t \to -\infty} y_0(t) = -\pi. \tag{2}$$

Physically, this solution is approximated by a pendulum which starts from rest very close to the upright vertical position and makes almost a complete rotation, coming again close to the vertical position.

Chaotic motion is not possible in this model, whatever the value of k. To obtain more erratic solutions we must add some sort of forcing term. This can take various forms, but the one we study here results from assuming that the support of the pendulum is subject to a vertical motion, up and down, which is sinusoidal. This adds a force proportional to $\sin \epsilon t$ to the gravitational force. We make the assumption that the force on the support varies slowly with time, and also that the damping force is small. This results in the equation

$$y'' + \epsilon\delta y' + (1 + \gamma \sin \epsilon t)\sin y = 0 \tag{3}$$

where δ and γ are fixed positive numbers and ϵ is positive but small. To avoid the delicate case where the coefficient of $\sin y$ can be zero, we require that $0 < |\gamma| < 1$. Equation (3) was studied by S. Wiggins, in **[16]**.

III. PREVIOUS RESULTS. To describe Wiggins' result, suppose that $y > 0$ represents displacement from rest in a counter-clockwise direction, and a full rotation occurs each time $y(t)$ crosses an odd multiple of π. He then shows that there is a $\Delta(\gamma) > 0$ such that the irregular behavior can occur if $0 \leq \delta < \Delta(\gamma)$ and ϵ is sufficiently small. We shall describe the function $\Delta(\cdot)$ shortly, but first let us specify the nature of this "irregular" behavior. Our measure of irregularity is that the pendulum makes a sequence of full rotations, alternating between clockwise and counter-clockwise rotations in an erratic manner. More precisely (without, however, yet specifying $\Delta(\gamma)$), we state this as a theorem.

Theorem 1 (Wiggins [16]). *Suppose that δ and γ are given numbers, with $0 < |\gamma| < 1$ and $0 \leq \delta < \Delta(\gamma)$. Then there is an $\epsilon_1 > 0$ such that for any ϵ with $0 < \epsilon < \epsilon_1$, and any finite or infinite sequence $\{m_j\}_{j=1,2,3,\ldots}$ of positive integers, there is a solution of (3) such that the corresponding motion consists of exactly m_1 full clockwise rotations, followed by exactly m_2 full counter-clockwise rotations, m_3 full clockwise rotations, and so forth. If the sequence is finite, then eventually the pendulum stops making full rotations.*

It is common to refer to the solutions corresponding to infinite non-repeating sequences as "chaotic," though, as we said, some researchers prefer a stricter interpretation of this term.

Wiggins obtains this striking result by applying the technique of Melnikov to the equation (3). This requires extending Melnikov's original method, because previously the forcing term was required to be "small" in amplitude, whereas here the small parameter measures the frequency of the oscillation, not its amplitude. The necessary extension was also given by Palmer **[12]**.

To define the function $\Delta(\cdot)$, Wiggins derives the appropriate "Melnikov" function for (3). While this concept has always seemed slightly mysterious to us, here it results from very standard energy methods involving the function $E(t)$. (See below.) Suppose that y_0 is the unique solution to (1) with $k = 0$ satisfying (2). Then

$$\Delta(\gamma) = |\gamma| \frac{\int_{-\infty}^{\infty} s y_0'(s) \sin y_0(s)\, ds}{\int_{-\infty}^{\infty} y_0'(s)^2\, ds}.$$

In other words, chaotic solutions exist for sufficiently small $\epsilon > 0$ if

$$\int_{-\infty}^{\infty} I_{y_0}(s)\, ds > 0, \tag{4}$$

where

$$I_y(s) = -\delta y'(s)^2 + |\gamma| s y'(s) \sin y(s). \tag{5}$$

The left side of (4) is the Melnikov function for the equation (3). Since y_0 satisfies (1) with $k = 0$, we can set $\sin y_0(s) = -y_0''(s)$ in the formula for $\Delta(\gamma)$, integrate by parts, and use the boundary conditions to obtain that $\Delta(\gamma) = \frac{1}{2}|\gamma|$.

IV. PROOF WHEN $\boldsymbol{\delta} = 0$. We will show how these results, and others, can be obtained by techniques which we feel are simpler than those used previously. Instead of studying Poincaré maps, we follow the solutions more directly, to determine how they vary as the initial conditions change. We need consider only initial conditions representing a pendulum which is released from a raised position, with zero initial velocity. The case $\delta = 0$ in (3) is particularly simple. Therefore we consider solutions to

$$y'' + (1 + \gamma \sin \epsilon t) \sin y = 0, \tag{6}$$

with initial conditions

$$y(0) = \alpha, \qquad y'(0) = 0. \tag{7}$$

Sometimes we will denote the solution by y_α. The goal is to obtain complicated solutions by adjusting α. This is sometimes called a "shooting method," because we attempt to "aim" the solution to get the desired behavior.

Shooting methods are topological, relying on separation theorems of some sort to distinguish between various types of behavior. As an example we prove a simple result about (6)–(7) which we will need later.

Lemma 1. *For sufficiently small $\epsilon > 0$ there is an $\hat{\alpha} \in (-\pi, 0)$ such that if $y = y_{\hat{\alpha}}$, then $y' > 0$ on $(0, \pi/2\epsilon]$ and $y(\pi/2\epsilon) = 0$. There is also an $\check{\alpha}$ such that $y' > 0$ on $(0, \pi/\epsilon]$ and $y(\pi/\epsilon) = 0$.*

Proof: We show how to get $\hat{\alpha}$; the argument for $\check{\alpha}$ is the same. If $-\pi < y < 0$, then $y'' > 0$, and so by choosing α in this range we ensure that $y' > 0$ as long as $y \leq 0$. Clearly, y crosses 0. Let

$$A = \left\{\alpha \in (-\pi, 0) |\ y(t) = 0 \text{ before } t = \frac{\pi}{2\epsilon}\right\}$$

and

$$B = \left\{\alpha \in (-\pi, 0) |\ y(t) = 0 \text{ after } t = \frac{\pi}{2\epsilon}\right\}.$$

Note that if $y(0) = -\pi$, $y'(0) = 0$, then y is constant, so that if α is very close to π, then y remains close to $-\pi$ for a long time before crossing 0. This shows that B is non-empty. To show that A is non-empty, consider a small negative α. As long as y is small, solutions of (6) are approximated by solutions of the linear equation $u'' + (1 + \gamma \sin \epsilon t)u = 0$. Solutions of this equation oscillate more quickly than solutions of $v'' + \sigma v = 0$ where $\sigma = 1 - |\gamma|$, and so cross zero in the interval $(0, \pi/\sqrt{\sigma})$. Hence if $2\epsilon < \sqrt{\sigma}$, then small negative α's lie in B.

The crossings of zero are with $y' > 0$, and so the continuity of solutions with respect to α implies that A and B are open sets. They are obviously disjoint, and the connectedness of the interval $(-\pi, 0)$ implies that there is a point in this interval which is not in A or B. Such an α gives the solution $y_{\hat{\alpha}}$ described in the lemma.

Note that we make no assertion about whether $\hat{\alpha} > \check{\alpha}$ or vice versa, nor will we need any such result. Comparisons of this kind are generally difficult to obtain. They are used in uniqueness proofs, but this is a paper about existence.

A crucial fact about solutions of (3) is that if $\alpha = k\pi$ for some integer k, then the solution is constant. In fact a stronger statement is true:

(i) If, for some t_0, $y(t_0) = k\pi$ and $y'(t_0) = 0$, then $y(t) = k\pi$ for all t.

This follows from the uniqueness theorem for initial value problems for ordinary differential equations. The solution $y \equiv k\pi$ is the unique solution satisfying the conditions $y = k\pi$, $y' = 0$ at the point $t = t_0$.

One reason that the case $\delta = 0$ is particularly simple is that in this case some solutions have certain symmetries, around points T_n/ϵ, where n is an integer and $T_n = (2n+1)\pi/2$. These are as follows.

(ii) If $y(T_n/\epsilon) = k\pi$ for some integer k, then

$$y\left(\frac{T_n}{\epsilon} + s\right) - k\pi = k\pi - y\left(\frac{T_n}{\epsilon} - s\right),$$

for all s.

(iii) If $y'(T_n/\epsilon) = 0$, then

$$y\left(\frac{T_n}{\epsilon} + s\right) = y\left(\frac{T_n}{\epsilon} - s\right)$$

for all s.

These are also proved by using the uniqueness of solutions to initial value problems. Note that the solution $y_{\hat{\alpha}}$ found in Lemma 1 is antisymmetric around $\pi/2\epsilon$, and therefore it increases up to π/ϵ, where it has a maximum in the region $0 < y < \pi$ and then starts to decrease.

The only detailed analysis required to prove Theorem 1 when $\delta = 0$ is used to obtain the following lemma.

Lemma 2. *For sufficiently small* $\epsilon > 0$, *there is some* $\underline{\alpha}$ *with* $-\pi < \underline{\alpha} < 0$, *such that* $y_{\underline{\alpha}}$ *increases monotonically on some interval* $[0, t_0]$ *and* $y_{\underline{\alpha}}(t_0) = \pi$.

The proof of Lemma 2 is quite simple in the situation we are considering. We give an outline below. Here we want to show how it is used in conjunction with a shooting technique to prove Theorem 1.

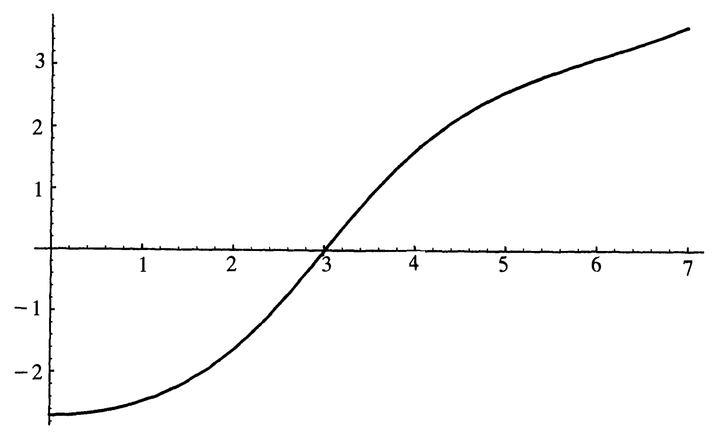


Figure 3. A graph of a solution behaving as described in Lemma 2.

Suppose that the first complete rotation of the pendulum is to be in the direction of positive y; i.e. we want the solution to cross $y = \pi$ before any possible crossing of $y = -\pi$. We begin by choosing $\alpha = \underline{\alpha}$ as in Lemma 2. The corresponding solution crosses $y = \pi$ at a point t_0, with $y' > 0$, and since $y'' > 0$ when $\pi < y < 2\pi$, there must be a $t_1 > t_0$ such that $y' > 0$ on $(0, t_1]$, and $y(t_1) = 2\pi$. Since $y'(t_1) > 0$, the implicit function theorem implies that there is a smooth function $t_1(\alpha)$, defined in a neighborhood of $\underline{\alpha}$ by the equation $y_\alpha(t_1(\alpha)) = 2\pi$.

However, recalling the properties of y in Lemma 1 when $\alpha = \hat{\alpha}$, we see that $t_1(\hat{\alpha})$ is not defined. Suppose for convenience that $\hat{\alpha} > \underline{\alpha}$. Then the function $t_1(\cdot)$ is continuous in some maximal interval of the form $[\underline{\alpha}, \bar{\alpha})$, where $\bar{\alpha} \leq \hat{\alpha} < 0$. Since $t_1(\cdot)$ can be extended continuously to an open neighborhood of any point where it is defined, we conclude that

$$\lim_{\alpha \to \bar{\alpha}-} t_1(\alpha) = \infty. \tag{8}$$

This result depends on property (i) above, for otherwise a crossing of 2π might disappear by the solution becoming tangent to this line for some α.

To illustrate the idea of the proof, suppose that $m_1 = 2$, so that we want y to cross 3π before recrossing π. This is accomplished by moving α from $\underline{\alpha}$ towards $\bar{\alpha}$. Since $t_1(\cdot)$ is continuous, it follows from (8) that there is an $\alpha_1 \in (\underline{\alpha}, \bar{\alpha})$ such that $t_1(\alpha_1) = T_{n_1}/\epsilon$, for some integer n_1. We now apply the anti-symmetry principle (ii). Since $y'(0) = 0$, $-\pi < y(0) < 0$, and y increases monotonically to reach 2π at T_{n_1}/ϵ, it must continue to increase monotonically until it crosses 3π and 4π, after which it has a maximum before any possible crossing of 5π. We have then accomplished the first step of achieving exactly two counter-clockwise rotations, and we next wish to obtain a clockwise rotation, since we are assuming that $m_2 \geq 1$.

Let $t_2(\alpha_1)$ be the first $t > 0$ where y_{α_1} has a local maximum. As we have noted, $4\pi < y_{\alpha_1}(t_2(\alpha_1)) < 5\pi$. Then $t_2(\cdot)$ can be extended as a continuous function in some neighborhood of α_1, as a solution of the equation $y'_\alpha(t) = 0$. As long as $t_2(\cdot)$ is continuous, $y_\alpha(t_2(\alpha))$ must lie in the interval $(4\pi, 5\pi)$, since (i) implies that the maximum cannot leave this interval by means of a tangency. Moreover, $t_2(\cdot)$ can be extended continuously to a maximum interval of the form $[\alpha_1, \bar{\alpha}_1)$, where $\alpha_1 < \bar{\alpha}_1 \leq \bar{\alpha}$, and

$$\lim_{\alpha \to \bar{\alpha}_1 -} t_2(\alpha) = \infty.$$

Therefore, we can find $\alpha_2 \in (\alpha_1, \bar{\alpha}_1)$ such that $t_2(\alpha_2) = T_{n_2}/\epsilon$, for some integer n_2. It is important to note that $t_1(\alpha_2)$ is not of the form T_n/ϵ, but it is still defined, as the first point where y_{α_2} crosses 2π. By (iii), y_{α_2} is symmetric around $t_2(\alpha_2)$, and so it must descend from its maximum there to recross 3π and π. If $m_2 = 2$ then this completes the second step of the induction process, since with the choice we have made of α_2, the next extremum of y_{α_2} is a minimum at $t = 2t_2(\alpha_2)$, where $y = y(0) \in (-\pi, 0)$. If $m_2 \neq 2$, we must adjust α further. As we adjust α, the various crossing points defined so far will change. However at each adjustment we only move α enough to bring the most recently defined crossing point or critical point to one of the points of symmetry or antisymmetry on the t axis. All the earlier such points remain bounded, and hence continuous in α, and none of the critical points can cross any line $y = k\pi$.

The case $m_2 = 5$ is typical. So far we have a solution which increases from its starting point in the interval $(-\pi, 0)$ past π and 3π, and then decreases back past 0. We can increase α still further so that this (downward) crossing of 0 is at one of

the points T_n/ϵ. Then the antisymmetry property (ii) shows that the solution must continue to decrease past $-\pi$ and -3π, but not past -5π.

This means the pendulum makes four counter-clockwise rotations, and we want exactly five. This is achieved by a further increase of α so that the point of antisymmetry is where the solution crosses $-\pi$. Since this is half-way between 3π and -5π, and the solution has a maximum in the earlier interval where it was between 4π and 5π, it will now have a minimum between -6π and -7π. It crosses -5π, but not -7π, which completes the second step.

Continuing this process, we obtain an increasing sequence of α's which is bounded above by $\bar{\alpha}$. This sequence must have a limit lying in the interval $(-\pi, 0)$, and this limiting value of α gives the solution we were after. Note that at each step, when we adjust α so that some crossing or extremal point lies at some odd multiple of $\pi/2\epsilon$, there are infinitely many choices of α, since there are infinitely many such odd multiples. This gives, for each sequence $\{m_i\}$, an infinite number of solutions of the desired type.

V. CHAOS AT PARTICULAR PARAMETER VALUES. It is apparent from the proof of Theorem 1 that, for $\delta = 0$, chaotic solutions exist if there is a solution such that $-\pi < y(0) < 0$, $y'(0) = 0$, and $y(T) = \pi$ for some $T > 0$. For particular parameter values this can be verified by following only one trajectory for a finite time interval. Therefore, in principle, rigorous estimates can be made which allow a proof that chaotic solutions exist for precise values of the parameters, rather than "for sufficiently small ϵ," as in Theorem 1. First we have to locate a good candidate for the parameter values. Standard numerical experimentation can easily be done on a personal computer, for example with the software Phsplan [4]. It is quickly determined that for $\epsilon = 0.1$, $\gamma = -0.5$, the solution with $y(0) = -2.7$, $y'(0) = 0$ increases monotonically until it crosses π, at approximately $t = 6.1$.

We then make use of a technique in numerical analysis called "interval arithmetic." In interval arithmetic, the computer is programmed to include error estimates in all arithmetic computations. An exposition is given in [1]. In addition to roundoff error it is necessary to allow for the truncation error introduced by the numerical method. Programs can be written to do this. We used PBASIC [1], which uses precise interval arithmetic, to do a completely rigorous integration of the equation with the parameter values and initial conditions found approximately using standard floating point computations. The result confirmed that the solution does indeed cross π, and therefore that with these parameter values there are solutions of arbitrary complexity, as described in the theorem.

VI. EXTENSIONS. The outline above of the proof of Theorem 1 makes it appear that symmetry is crucial for this result. But this is misleading. Symmetry considerations shorten the proof, but the heart of our method is the topological shooting principle. This is fortunate, for as soon as we add a damping term, as in (3), properties (ii) and (iii) do not hold. Shooting works because (i) is still valid. We need a slight extension of Lemma 2, but this is not difficult.

Physical intuition may cause doubts about this, because damping reduces energy and tends to stop the complete rotations. However the oscillation of the support can add energy if it is timed correctly. It is rather like pushing a child's swing. If the pushes occur in the direction of motion, the swing will go higher, despite air resistance. If the resisting forces are not too high we can indeed push a swing over the top, (though perhaps the child will be better off if we do not). Do not carry this analogy too far, however. A very important difference is that in our case the

motion of the support is determined ahead of time, and not adjusted to fit the motion of the pendulum.

In fact, even the periodicity of the forcing is not required. We can consider more general equations

$$y'' + \epsilon\delta y' + p(\epsilon t)\sin y = 0 \tag{9}$$

where the positive smooth function p increases and decreases in some fashion. For example, here is a set of sufficient conditions on p.

(a) p, $1/p$, p' and p'' exist and are bounded on $[0, \infty)$.

(b) There are sequences $\{t_j\}$ and $\{\tau_j\}$ tending to infinity and a $c > 0$ such that $p'(t_j) \geq c$ and $p'(\tau_j) \leq -c$.

This includes almost periodic functions and many others, and goes beyond what has been found using Poincaré maps, for it is difficult to define such a map usefully when the equation depends explicitly on time in an irregular fashion.

The damping term $\epsilon\delta y'$ in (9) is responsible for the introduction of the Melnikov function as described earlier. This enters into the proof of Lemma 2 when $\delta > 0$, but plays no role in the shooting part of the argument. We conclude this paper with a brief discussion of how to prove Lemma 2.

VII. OUTLINE OF PROOF OF LEMMA 2. The basic idea is to consider the energy $E(t)$, as defined earlier. The damping term tends to reduce E (makes $E' < 0$ when $y' \neq 0$), while the oscillation in the support may increase or decrease E, depending on the relative direction of movement of the support and the pendulum at any given time. Suppose again that $\delta = 0$ and $p(s) = 1 + \gamma \sin s$. We find using (6) that $E'(t) = -\gamma y'(t)\sin \epsilon t \sin y(t)$. To prove Lemma 2, we show that the initial position α can be adjusted so that $E(t)$ increases enough during the first swing to get the pendulum "over the top" for one complete revolution.

Suppose that $\gamma > 0$. Then we can choose $\alpha = \check{\alpha}$, which was found in Lemma 1. In this case we have $\sin \epsilon t > 0$ and $\sin y < 0$ in the interval $(0, \pi/\epsilon)$, and both of these quantities change sign at this point. It follows that E increases on the entire interval $(0, 2\pi/\epsilon)$, as long as $y' > 0$, $y < \pi$.

We can extimate the change in E while $y' > 0$, $y < \pi$ as follows. If $\pi/\epsilon \leq t \leq 2\pi/\epsilon$, then

$$\begin{aligned} E(t) &= E(0) + \int_0^t \{-\gamma y'(s)\sin \epsilon s \sin y(s)\}\, ds \\ &> E(0) + \int_{\pi/\epsilon - 1}^{\pi/\epsilon} \{-\gamma y'(s)\sin \epsilon s \sin y(s)\}\, ds. \end{aligned} \tag{10}$$

The second term on the right is estimated by proving a simple lemma showing that as $\epsilon \to 0$, the solution y found in Lemma 1 must tend to $y_0(t - \pi/\epsilon)$, where y_0 is the unique solution of (1)–(2) with $k = 0$. That is, for example,

$$\max_{\pi/\epsilon - 1 \leq t \leq \pi/\epsilon} \left| y(t) - y_0\left(t - \frac{\pi}{\epsilon}\right) \right| \to 0.$$

Setting $s - \pi/\epsilon = \sigma$, and noting that $\sin \epsilon\sigma \to \epsilon\sigma$ uniformly on compact σ-intervals, we find that the second term on the right of (10) is asymptotically like $\int_{-1}^{0} \gamma\epsilon\sigma y_0'(\sigma)\sin y_0(\sigma)\, d\sigma = \mu\epsilon$ where μ is a positive number. We also need an easy estimate for $E(0) = -\cos \check{\alpha}$. Without going into further details, this enables us to obtain quickly an estimate of the form $y'(t) \geq k\sqrt{\epsilon}$ for $t \geq \pi/\epsilon$, implying that y rises above π before $t = 2\pi/\epsilon$.

When δ is positive, the rate of change of energy is given by $E'(t) = -\delta\epsilon y'^2 - \gamma y' \sin \epsilon t \sin y$. The first term causes E to decrease, while the sign of the second

term alternates. The analysis of the net change of E in the same situation as above, where $y = 0$ when $t = \pi/\epsilon$, is a little more complicated and leads to a consideration of the Melnikov function. The case of a non-periodic forcing is no harder; periodicity is irrelevant to Lemma 2.

VIII. FINAL REMARKS. Theorem 1 and the extensions described in the last section by no means tell the whole story, even for (6). While we show that there is an uncountable number of erratic solutions, our numerical simulations indicate that most solutions eventually settle down into small oscillations around an even multiple of π, which represents the downward vertical position of the pendulum. We do not know of a proof of this, however.

Also, we do not know whether the results can be extended to include larger values of ϵ. Our standard numerical computations (not rigorous) show that the crucial solution of Lemma 2 exists at least out to $\epsilon = 50$. For very large ϵ it seems that another subtle effect enters in, the so-called "exponential splitting of separatrices" [**5**]. This is certainly beyond the scope of this paper. What we would like to show is that the phenomenon occurs for all values of ϵ, and this seems to require some new estimates.

REFERENCES

1. O. Aberth, *Precise Numerical Analysis*, William C. Brown Publishers, Dubuque, Iowa, 1988.
2. F. Brauer and J. Nohel, *Introduction to Differential Equations with Applications*, Harper and Row, 1985.
3. R. L. Devaney, *Chaotic Dynamical Systems*, Addison Wesley, 1989, 2nd edition.
4. G. B. Ermentrout, *PhasePlane, the Dynamical Systems Tool*, Brooks/Cole Publishing, Pacific Grove, CA, 1990.
5. E. Fontich and C. Simó, The Splitting of Separatrices for Analytic Diffeomorphisms, *Ergodic Theory and Dynamical Systems* 10 (1990), 295–318.
6. J. Guckenheimer and P. Holmes, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields*, Springer-Verlag (NY), 1982.
7. S. Hastings and J. B. McLeod, On the Periodic Solutions of a Forced Second-Order Equation, to appear in *Nonlinear Science*.
8. S. Hastings and W. Troy, Oscillating Solutions of the Falkner-Skan Equation for Positive β, *J. Diff. Eqns.* 71 (1988), 123–144.
9. Y. Li and J. Yorke, Period Three Implies Chaos, *American Mathematical Monthly* 82 (1975), 985–992.
10. E. N. Lorenz, Deterministic Non-periodic Flow, *J. Atmospheric Sci.* 20 (1963), 130–141.
11. V. K. Melnikov, On the Stability of the Center for Time Periodic Solutions, *Trans. Moscow Math. Soc.* (Trudy), 12 (1963), 3–52.
12. K. J. Palmer, Transversal Heteroclinic Points and Cherry's Example of a Nonintegrable Hamiltonian System, *J. Diff. Eqns* 65 (1986), 321–360.
13. A. N. Sharkovsky, Coexistence of Cycles of a Continuous Map of a Line into itself, *Ukrainian Math. J.* 16 (1964), 61–71.
14. L. P. Shil'nikov, On the Generation of a Periodic Motion from Trajectories Doubly Asymptotic to an Equilibrium State of Saddle Type, *Math. USSR-Sb.* 6 (1968), 427–438.
15. S. Smale, Diffeomorphisms with Many Periodic Points, *Differential and Combinatorial Topology*, Princeton Univ. Press, Princeton, NJ, 1965, 63–80.
16. S. Wiggins, On the Detection and Dynamical Consequences of Orbits Homoclinic to Hyperbolic Periodic Orbits and Normally Hyperbolic Invariant Tori in a Class of Ordinary Differential Equations, *SIAM J. Appld. Math.* 48 (1988), 262–285.

Department of Mathematics & Statistics
University of Pittsburgh
Pittsburgh, PA 15260
sph@mthsn4.math.pitt.edu

An Application for the Curiosity $(\log_x N)'$

David A. Wagstaff, Theodore A. Norman, and Douglas M. Campbell

Students often believe that differentiation formulas such as

$$(*) \qquad [\log_x N]' = -(\log_x N)/(x \ln x)$$

are mere curiosities. We present a practical application of $(*)$.

In practice, unsorted data files on a hard disk may be extremely large (e.g. 40 megabytes), while available RAM (Random Access Memory) on many personal computers is small (e.g. 1 megabyte). There is a simple strategy to sort such a file:

1. Divide it into chunks which are the size of RAM (for our example, 1 megabyte chunks). For each chunk, read the chunk into RAM, sort it by one's favorite internal sort, and write the chunk back to the hard disk as a separate file (see [**1**], p. 263–p. 270; [**2**] chapter 5.4, Theorem L, page 371).

2. Then, as FIGURE 1 indicates, groups of x of these sorted chunks are merged into a larger sorted chunk, and written back to the hard disk. This continues until the final merge, in which only x huge chunks remain and they are merged into the final sorted file.

Although this example is a considerable simplification of the real problem, the most time consuming part of this operation is the *seek*, in which the access mechanism of the hard disk is moved to the proper track on the hard disk to read the information. The question arises, what value of x will minimize the number of seeks? Furthermore, how does the value of x depend on the file size and the available RAM?

Theorem. *Let a file have N records and let the computer's RAM hold M records. The value of x to minimize the number of seeks in an x-way merge is* 3, *independent of N and M.*

Proof: Sub-divide the N records into $R = N/M$ files (chunks), which are read into memory, internally sorted, and written to the hard disk to form the top row of Figure 1. (By adding specially marked dummy records, we may assume that R is a power of x.) The system of x-way merges of Figure 1 has $\log_x R$ levels. At each level, the contents of the original file have to be read into x buffers. Since RAM can only hold M records, each of the x buffers holds M/x records. Each time a buffer is filled, a seek is required. Therefore, the number of seeks per level is $N/(M/x)$ which is xR. The total number of seeks, y, is the number of seeks per level times the number of levels:

$$y = xR \log_x R.$$

Taking the derivative with respect to x we see that $y' = R \log_x R[-1 + \ln x]/\ln x$, which is zero when $x = e$. Since y' goes from negative to positive at $x = e$, the function y has its minimum at $x = e$, independent of N and M. But the

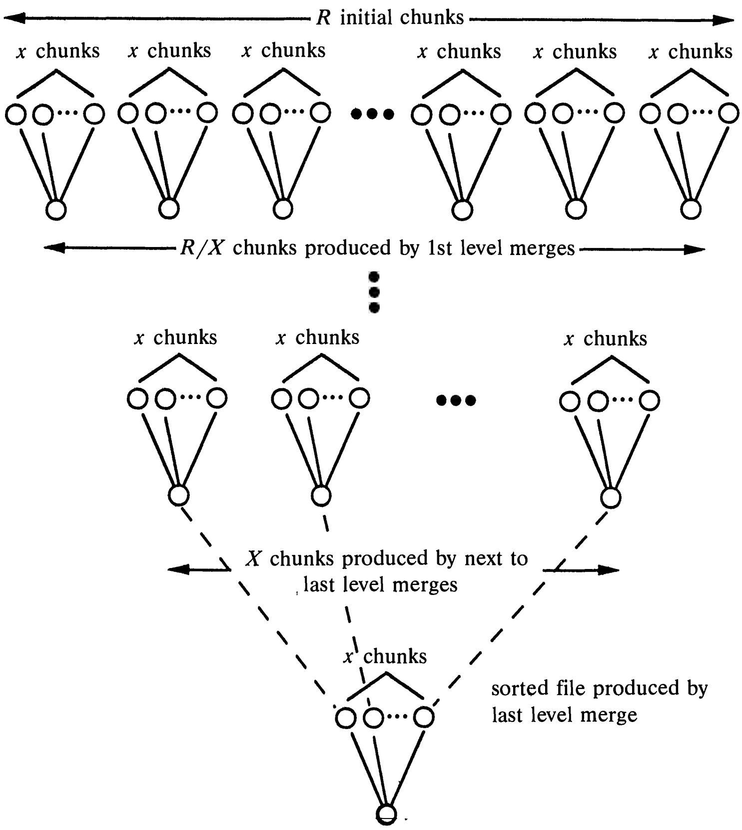


Figure 1

value of x in an x-way merge must be an integer. Writing R as 2^z, for some $z > 0$, we note that

$$\begin{aligned} y(2) - y(3) &= 2R\log_2 R - 3R\log_3 R \\ &= R(2z - 3z\log_3 2) \\ &= Rz(\log_3 9 - \log_3 8), \end{aligned}$$

which confirms that a 3-way merge minimizes the number of seeks.

To derive $(*)$, we note that $y = \log_x N$ can be rewritten as $x^y = N$ and thereby as $y \ln x = \ln N$. Taking the derivative yields $y' \ln x + y/x = 0$, which when solved for y' yields $(*)$.

REFERENCES

1. Michael J. Folk, Bill Zoellick, "File Structures: A Conceptual Toolkit", Addison-Wesley, Reading, Mass, 1987.
2. Donald E. Knuth, "The Art Of Computer Programming, Volume 3, Sorting and Searching", Addison-Wesley, Reading, Mass, 1973.

Computer Science Department
Brigham Young University
Provo, UT 84602
campbell@cs.byu.edu

Vandermonde Strikes Again

Miriam Schapiro Grosof and Geraldine Taiani

The search for "cute" proofs—those in which arguments or techniques that at first glance appear completely unrelated in substance are used to establish familiar results—provides healthful exercise for both students and experts. One of the more versatile tools for this purpose is the Vandermonde matrix and its determinant. This mathematical object has an honorable history dating from the late 18th century [**1**] and has enjoyed sporadic revivals of interest [**3**], [**5**]. In the past, most undergraduate major courses included its applications in the proof that values at $n + 1$ distinct points uniquely determine a monic polynomial of degree n [**7**] and in the definition of the signature of a permutation [**4**]. We present here a novel, indeed unexpected, application of the Vandermonde.

A theorem of Abel [**2**] states: *if $P(x), Q(x)$ are any two polynomials such that* $\deg Q = n \geq 3$, *Q has no multiple roots, and* $\deg P = m \leq n - 2$, *then*

$$\text{(A)} \sum \frac{P(r_i)}{Q'(r_i)} = 0$$

where the summation is over all n distinct roots r_i of Q. (As usual, Q' denotes the derivative of Q.)

Abel's original proof (of a more complicated result) uses integrals. The modern standard proof is based on residue theory. Since $\deg P \leq \deg Q - 2$,

$$\left| \int_{|z|=R} \frac{P(z)}{Q(z)}\, dz \right| \leq \frac{C}{R} \quad \text{for some constant } C > 0 \text{ and } R \text{ sufficiently large;}$$

hence

$$\lim_{R \to \infty} \int_{|z|=R} \frac{P(z)}{Q(z)}\, dz = 0.$$

However,

$$\int_{|z|=R} \frac{P(z)}{Q(z)}\, dz = 2\pi i \cdot \left(\text{sum of residues of } \frac{P(z)}{Q(z)} \text{ inside } |z| < R \right),$$

and since $P(z)/Q(z)$ has simple poles at the roots of Q the residues of $P(z)/Q(z)$ inside $|z| = R$ are precisely

$$\left\{ \frac{P(r_i)}{Q'(r_i)}, r_i \text{ roots of } Q \text{ in } |z| = R \right\}.$$

The desired (A) follows.

We have found an algebraic proof of (A) in the spirit of classical theory of equations. Strictly speaking it requires no complex analysis. Given polynomial

Q with $\deg Q = n \geq 3$ and distinct (real or complex) roots $r_1, r_2, \ldots, r_n$, assume w.l.o.g. Q is monic so $Q(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$. Then $Q'(x) = \Sigma_i (x - r_1)(x - r_2) \cdots \widehat{(x - r_i)} \cdots (x - r_n)$, that is, each summand has one factor, $(x - r_i)$, omitted. Thus,

$$\begin{aligned} Q'(r_i) &= (r_i - r_1)(r_i - r_2) \cdots (r_i - r_{i-1})(r_i - r_{i+1}) \cdots (r_i - r_n) \\ &= (-1)^{n-i}(r_i - r_1)(r_i - r_2) \cdots (r_i - r_{i-1})(r_{i+1} - r_i) \cdots (r_n - r_i) \\ &= (-1)^{n-i} \frac{\prod\limits_{j>k} (r_j - r_k)}{\prod\limits_{\substack{j>k \\ j,k \neq i}} (r_j - r_k)}. \end{aligned}$$

Recall now the Vandermonde determinant [6]

$$V_n(a_1, \ldots, a_n) = \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & & & \\ a_1^{n-2} & a_n^{n-2} & \cdots & a_n^{n-2} \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{bmatrix}$$

is a polynomial of degree $n(n-1)/2$ in the n variables $a_1, \ldots, a_n$; it can be written as the product $(a_2 - a_1) \cdots (a_n - a_{n-1}) = \prod_{j>k}(a_j - a_k)$. $V_n(a_1, \ldots, a_n) = 0$ if and only if $a_k = a_j$ for some $k \neq j$. Moreover, the minors of entries in row n are themselves Vandermondes: in particular, the minor of a_i^{n-1} is $V_{n-1}(a_1, \ldots, \hat{a}_i, \ldots, a_n)$ which is precisely $\prod_{j>k,\, j,\, k \neq i}(a_j - a_k)$. Hence,

$$Q'(r_i) = (-1)^{n-i} \frac{V_n(r_1, \ldots, r_n)}{V_{n-1}(r_1, \ldots, \hat{r}_i, \ldots, r_n)}.$$

Now given polynomial P with $0 \leq m = \deg P \leq n - 2$

$$\begin{aligned} \sum_i \frac{P(r_i)}{Q'(r_i)} &= \sum_i (-1)^{n-i} P(r_i) \frac{V_{n-1}(r_1, \ldots, \hat{r}_i, \ldots, r_n)}{V_n(r_1, \ldots, r_n)} \\ &= \frac{(-1)^{n-1}}{V_n(r_1, \ldots, r_n)} \sum_i (-1)^{i-1} P(r_i) V_{n-1}(r_1, \ldots, \hat{r}_i, \ldots, r_n) \\ &= \frac{(-1)^{n-1}}{V_n(r_1, \ldots, r_n)} \cdot (-1)^{n-1} \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_n \\ \vdots & \vdots & & \\ r_1^{n-2} & r_2^{n-2} & \cdots & r_n^{n-2} \\ P(r_1) & P(r_2) & & P(r_n) \end{bmatrix}. \end{aligned}$$

However, $P(x)$ has degree $\leq n - 2$ so that each $P(r_i)$ is the same linear combination of $1, r_i, r_i^2, \ldots, r_i^{n-2}$ and hence the determinant is zero, as desired.

Note that this result (and Abel's proof but not ours) is true when $n = 2$, $m = 0$; $n = 2$, $P \equiv 0$; or $n = 1$, $P \equiv 0$. These cases are easily proved by differentiation and substitution in (A).

We have noticed that recent texts ignore the Vandermonde so that even our advanced students have never heard of it, nor its discoverer, nor indeed the entire category of problems which drove the work of Lagrange, Galois, Abel and their heirs. The topic (along with the rest of theory of equations, now "lost") is well suited to independent study, a mini-course or a special project, if there is no room for it in the modern over-crowded pregraduate major sequence.

We wish to thank the referee for a useful comment.

REFERENCES

1. Florian Cajori, *A History of Mathematics*, (ed. 2), Macmillan, NY, 1919, p. 266.
2. P. Griffiths, Variations on a theorem of Abel, *Inventiones* 35 (1976), 321–390.
3. Allen Klinger, The Vandermonde matrix, *Am. Math. Monthly* 74 (1967), 571–574.
4. Lowell J. Paige, and J. Dean Swift, *Elements of Linear Algebra*, Ginn & Co., Boston, 1961, p. 109.
5. Joseph J. Rushanan, On the Vandermonde matrix, *Am. Math. Monthly* 96 (1989), 921–924.
6. J. V. Uspensky, *Theory of Equations*, McGraw-Hill, NY, 1938, p. 214.
7. Louis Weisner, *Introduction to the Theory of Equations*, Macmillan, NY, 1938, p. 56.

Department of Mathematics
Yeshiva University
New York, NY 10016

Department of Mathematics
Pace University
New York, NY 10038

More on pi

I may well have made a mistake in my note *How to Make Pi Equal to Three* in the February 1992 issue of this *Monthly*, but it was not the mistake that Professor Dario Castellanos points out in his recent letter (*Monthly*, January 1993), because I did not take my ruler aboard the spinning circle.

Professor Castellanos takes a ruler on board a spinning circle, and uses it to measure the circumference of a stationary circle. Naturally, he gets a value of π greater than usual.

I used a stationary ruler to measure the circumference of a spinning circle, so I got a value of π less than usual.

The trouble is I used special relativity instead of general relativity. A spinning circle is an accelerated system, which calls for general relativity. I assumed that for large radius we could approximate circular motion with straight line motion, and proceeded accordingly.

But I never took my ruler on board the spinning circle.

Along these same lines, here is a paradox I cannot explain. Suppose a train on a circular track is so long that reaches all the way around, and the caboose is hitched to the locomotive. If the train travels near the speed of light, each car decreases in length, so we have a short train filling a long track. What happens?

—*Rick Norwood*
Department of Mathematics
East Tennessee State University
Johnson City TN 37614

NOTES

Edited by: **John Duncan**

Embedding Countable Groups in 2-Generator Groups

Fred Galvin

The aim of this note is to popularize a simple proof, due to Neumann and Neumann [**5**], of the fact that every countable group is embeddable in a 2-generator group. This was first proved by Higman, Neumann, and Neumann [**2**, Theorem IV] and (independently) Freudenthal [**2**, p. 254], using free products with amalgamations. The proof given by Neumann and Neumann [**5**] used wreath products, which are widely regarded as no less terrifying than free products with amalgamations. I am indebted to Professors A. M. W. Glass, G. Higman, and P. M. Neumann, each of whom pointed out (in response to an earlier version of this note) that the Neumann-Neumann proof is really quite simple, and that it can easily be expressed directly in terms of permutations. Here, then, is a short proof that assumes no more background than is needed to understand the statement of the theorem.

As usual, $\mathbb{Z}$ is the set of integers and $\mathbb{N}$ is the set of natural numbers; $\langle a, b\rangle$ is the group generated by a and b; $\mathrm{Sym}(\Omega)$ is the group of all permutations of a set Ω; permutations are regarded as right operators, and are composed from left to right.

Theorem 1. *Every countable group is embeddable in a 2-generator group.*

Proof: Consider a countable group $G = \{g_1, g_3, g_5, \dots\}$; the elements are indexed by odd positive integers. We may assume that G is a subgroup of $\mathrm{Sym}(\mathbb{N})$. Define permutations a and b in $\mathrm{Sym}(\mathbb{Z} \times \mathbb{Z} \times \mathbb{N})$ by setting $(m, n, p)a = (m+1, n, p)$ and

$$(m,n,p)b = \begin{cases} (m, n+1, p) & \text{if } m = 0; \\ (m, n, pg_m) & \text{if } m \text{ is odd, } m > 0,\ n \geq 0; \\ (m, n, p) & \text{otherwise.} \end{cases}$$

Let $b_i = a^i b a^{-i}$ and $\hat{g}_i = b_i b^{-1} b_i^{-1} b$ for $i = 1, 3, 5, \dots$. Straightforward (if slightly tedious) calculation shows that $(m, n, p)\hat{g}_i = (0, 0, pg_i)$ if $m = n = 0$, while $(m, n, p)\hat{g}_i = (m, n, p)$ otherwise. Thus $\hat{G} = \{\hat{g}_i\colon i = 1, 3, 5, \dots\}$ is a subgroup of $\langle a, b\rangle$ isomorphic to G.

It may have occurred to the reader to wonder whether Theorem 1 can be proved by just showing that any countable subgroup of a symmetric group $S = \mathrm{Sym}(\Omega)$ is contained in a 2-generator subgroup of S. In fact, this was a question of Wagon [**8**]. An old theorem of Sierpiński [**7**, **9**] says that any countable set of

selfmaps of an infinite set Ω is contained in the semigroup generated by two selfmaps of Ω; Wagon asked whether one could replace "selfmaps" by "permutations" in Sierpiński's theorem. The answer is yes [**1**], but the proof is a bit more involved and will appear elsewhere.

The two generators in the proof of Theorem 1 were both of infinite order. B. H. Neumann [**4**, p. 541] remarked that every countable group is embeddable in a 2-generator group with generators of prescribed orders $q \geq 8$ and $r \geq 2$; this was improved by Levin [**3**] to $q \geq 3$ and $r \geq 2$, which is the best possible result in this direction. The proof of Levin's result is a little too complicated to give here; however, we can get two generators of finite order by modifying the proof of Theorem 1. We need the following easy lemma:

Lemma 1 [**6**, Exercise 10.1.17, p. 259]. *Every permutation is the product of two involutions.*

Proof: It suffices to consider the case of a permutation consisting of a single (finite or infinite) cycle. Note, e.g., that a 6-cycle is obtained by multiplying the involutions $(1,2)(3,4)(5,6)$ and $(2,3)(4,5)$. This example can easily be generalized to get cycles of any desired length.

Theorem 2. *Every countable group is embeddable in a 2-generator group with one generator of order* 11 *and the other of order* 2.

Proof: Let G be a countable group. We may assume that G is a subgroup of $\mathrm{Sym}(\mathbb{N})$; moreover, by Theorem 1 and Lemma 1, we may assume that G is generated by four involutions, which we call g_3, g_5, g_7, and g_9. Define permutations a and b in $\mathrm{Sym}(\mathbb{Z}_{11} \times \mathbb{Z} \times \mathbb{N})$, of orders 11 and 2 respectively, by setting $(m,n,p)a = (m+1,n,p)$ and

$$(m,n,p)b = \begin{cases} (m, n+(-1)^n, p) & \text{if } m = 0; \\ (m, n-(-1)^n, p) & \text{if } m = 1; \\ (m, n, pg_m) & \text{if } m \in \{3,5,7,9\},\ n \equiv 0 \pmod 4,\ n \geq 0; \\ (m,n,p) & \text{otherwise.} \end{cases}$$

Let $c = (baba^{-1})^2$. Note that $(0,n,p)c = (0, n + 4(-1)^n, p)$, while $(m,n,p)c = (m,n,p)$ if $m \neq 0$. Let $b_i = a^i b a^{-i}$ and $\hat{g}_i = b_i c^{-1} b_i c$ for $i = 3,5,7,9$. Then $(m,n,p)\hat{g}_i = (0,0,pg_i)$ if $m = n = 0$, while $(m,n,p)\hat{g}_i = (m,n,p)$ otherwise. Hence $\langle \hat{g}_3, \hat{g}_5, \hat{g}_7, \hat{g}_9 \rangle$ is a subgroup of $\langle a, b \rangle$ isomorphic to G.

Theorem 3. *Every countable group is embeddable in a 2-generator group with one generator of prescribed order $q \geq 5$ and the other of order* 2.

Proof: By Theorem 2 and Lemma 1, we may assume that the given countable group is a subgroup of $\mathrm{Sym}(\mathbb{N})$ generated by three involutions, which we call g_2, g_3, and g_4. Define permutations a and b in $\mathrm{Sym}(\mathbb{Z}_q \times \mathbb{Z} \times \mathbb{N})$, of orders q and 2

respectively, by setting $(m, n, p)a = (m + 1, n, p)$ and

$$(m,n,p)b = \begin{cases} (m, n + (-1)^n, p) & \text{if } m = 0; \\ (m, n - (-1)^n, p) & \text{if } m = 1; \\ (m, n, pg_2) & \text{if } m = 2,\ n \equiv 0 \pmod{24},\ n \geq 0; \\ (m, n, pg_3) & \text{if } m = 3,\ n \equiv 8 \pmod{24},\ n \geq 0; \\ (m, n, pg_4) & \text{if } m = 4,\ n \equiv 16, \pmod{24},\ n \geq 0; \\ (m, n, p) & \text{otherwise.} \end{cases}$$

Let $c = (baba^{-1})^4$; then $(0, n, p)c = (0, n + 8(-1)^n, p)$, while $(m, n, p)c = (m, n, p)$ if $m \neq 0$. Let $b_i = a^i b a^{-i}$ and $\hat{g}_i = c^{i-2} b_i c^{-3} b_i c^{5-i}$ for $i = 2, 3, 4$; then $(m, n, p)\hat{g}_i = (0, 0, pg_i)$ if $m = n = 0$, while $(m, n, p)\hat{g}_i = (m, n, p)$ otherwise.

ACKNOWLEDGMENTS. I thank the editor and referee for their encouragement and advice.

REFERENCES

1. Fred Galvin, Generating countable sets of permutations, *Abstracts Amer. Math. Soc.* 13 (1992), 509.
2. Graham Higman, B. H. Neumann, and Hanna Neumann, Embedding theorems for groups, *J. London Math. Soc.* 24 (1949), 247–254.
3. F. Levin, Factor groups of the modular group, *J. London Math. Soc.* 43 (1968), 195–203.
4. B. H. Neumann, An essay on free products of groups with amalgamations, *Philos. Trans. Roy. Soc. London Ser.* A246 (1954), 503–554.
5. B. H. Neumann and Hanna Neumann, Embedding theorems for groups, *J. London Math. Soc.* 34 (1959), 465–479.
6. W. R. Scott, *Group Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1964.
7. W. Sierpiński, Sur les suites infinies de fonctions définies dans les ensembles quelconques, *Fund. Math.* 24 (1935), 209–212.
8. Stan Wagon, personal communication, 1979.
9. Composition of functions (solution of Problem 6244, proposed by John Myhill), *Amer. Math. Monthly* 87 (1980), 676–678.

Department of Mathematics
University of Kansas
Lawrence, KS 66045-2142

Abelian Forcing Sets

Joseph A. Gallian and Michael Reid

Many readers of the MONTHLY have encountered particular cases of the following question. Suppose G is a group and n is an integer with the property that $(ab)^n = a^n b^n$ for all a and b in G. Which values of n imply that G is Abelian? Indeed, standard exercises in undergraduate abstract algebra textbooks ([**1**], [**2**], [**3**], [**4**]) are to show that $n = 2$ and $n = -1$ are two such values. Are there others? If $n \in Z$, we say that a group G is *n-Abelian* if $(xy)^n = x^n y^n$ for all $x, y \in G$. Thus

our question may be reformulated as "for which integers n is an n-Abelian group necessarily abelian?" If p is any prime, consider the non-Abelian group

$$G_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in Z_p \right\}.$$

If p is odd, then $x^p = e$ for all $x \in G_p$. We say that a group G *has exponent* n if $x^n = e$ for all $x \in G$. Thus, G_p has exponent p. Also, G_2 (which is isomorphic to the group of symmetries of a square) has exponent 4. Note that if G is a group with exponent n, then for any integer k, G is kn-Abelian and $(kn + 1)$-Abelian. The examples G_p are now sufficient to show that the only integers n for which n-Abelian implies Abelian are $n = 2$ and $n = -1$. Indeed, for p odd, G_p is pk-Abelian and $(pk + 1)$-Abelian for any integer k, while G_2 is $4k$-Abelian and $(4k + 1)$-Abelian.

More generally, let us call a set of integers T *Abelian forcing* if whenever G is a group with the property that G is n-Abelian for all n in T, then G is Abelian. So far we have seen that the only singleton Abelian forcing sets are $\{-1\}$ and $\{2\}$. What about other sets? Both of Herstein's algebra textbooks ([**3**, p. 31] and [**4**, p. 57]) include the exercise that sets containing three consecutive integers are Abelian forcing. Moreover, one of Herstein's books ([**4**, p. 57]) has an exercise that $\{3, 5\}$ is an Abelian forcing set. In contrast, the set $\{3, 7\}$ is not Abelian forcing, as G_3 is both 3-Abelian and 7-Abelian.

What characterizes the Abelian forcing sets? Although we could not find the answer to this precise question in the literature, some of the essential features of our argument below can be gleaned from a paper by F. Levi [**5**] written in the group-theoretic language of fifty years ago. (Levi investigated the question of when the mapping $a \mapsto a^n$ is a group endomorphism.) Our formulation of the question, the answer and the proof make the material more accessible to undergraduates.

Theorem. *A set T of integers is Abelian forcing if and only if the greatest common divisor of the integers $n(n-1)$ as n ranges over T is* 2. (*Note that each $n(n-1)$ is even.*)

Proof: The necessity of the condition again follows from the examples G_p. For p prime, let $T_p = \{n \in Z | 2p \text{ divides } n(n-1)\}$. Then for p odd, $T_p = \{pk, pk+1 | k \in Z\}$, while $T_2 = \{4k, 4k+1 | k \in Z\}$. From our earlier observation, G_p is n-Abelian for each $n \in T_p$, so T_p is not Abelian forcing. This proves necessity.

To prove sufficiency of the condition, suppose that $T \subseteq Z$ satisfies $\gcd(n(n-1) | n \in T) = 2$, and G is a group which is n-Abelian for all $n \in T$. Let $S = \{n \in Z | G \text{ is } n\text{-Abelian}\}$, so that $T \subseteq S$. First note that if $m, n \in S$, then $mn \in S$. Also, if $n \in S$, then for any $x, y \in G$, we have $(xy)^n = x^n y^n$, so that $(yx)^{n-1} = x^{n-1}y^{n-1}$, whence $(yx)^{1-n} = y^{1-n}x^{1-n}$. Thus, if $n \in S$, then $1 - n \in S$. Since $n = 1 - (1 - n)$, the converse holds as well.

Our main difficulty at this point is that S is not closed under addition. However, suppose that $n \in S$ has the property that $x^n \in Z(G)$ (the center of G) for all $x \in G$. Then, for arbitrary $m \in S, x, y \in G$, we have $(xy)^{m+n} = (xy)^m(xy)^n = x^m y^m x^n y^n = x^m x^n y^m y^n = x^{m+n}y^{m+n}$, so $m + n \in S$.

This motivates the definition $R = \{n \in S | x^n \in Z(G) \text{ for all } x \in G\}$. It is easy to see that $n \in R$ if and only if $-n \in R$. Thus, from our previous remark, R is an additive subgroup of Z. We now claim that if $n \in S$, then $n(n-1) \in R$. We do this in several steps.

Note that if $n \in S$, then $1 - n \in S$, so $n(1-n) \in S$. For arbitrary $x, y \in G$, we have $yx^n y^n y^{-1} = y(xy)^n y^{-1} = (yx)^n = y^n x^n$, so that $y^{1-n}x^n = x^n y^{1-n}$. Thus n-th powers commute with $(1-n)$-th powers. Now, for any $x \in G$, $x^{n(1-n)}$ is both an n-th power and a $(1-n)$-th power. Thus, for any $y \in G$, $x^{n(1-n)}$ commutes with both y^n and y^{1-n}, and therefore also with y. This shows that $x^{n(1-n)} \in Z(G)$, so that $n(1-n)$ and thus, also, $n(n-1)$ are in R.

We are now in position to prove sufficiency. Since the greatest common divisor of the numbers $n(n-1)$ for $n \in T$ is 2, the additive subgroup R of Z contains 2. Therefore, G is 2-Abelian, and thus Abelian. This proves sufficiency.

Finally, to see that $\{n, n+1, n+2\}$ is Abelian forcing, note that $n(n-1) - 2(n+1)n + (n+2)(n+1) = 2$, so that

$$gcd(n(n-1), (n+1)n, (n+2)(n+1)) = 2.$$

The authors recently discovered that the problem addressed here appeared as a problem in the MONTHLY in 1974 (E2411, vol. 81, page 410). It is also a special case of a result of L. C. Kappe, "On n-Levi groups", *Arch. Math.*, 47 (1986) 198–210.

REFERENCES

1. J. B. Fraleigh, *A First Course in Abstract Algebra*, 4th ed., Addison-Wesley, Reading, MA, 1989.
2. J. A. Gallian, *Contemporary Abstract Algebra*, 2nd ed., D.C. Heath, Lexington, MA, 1990.
3. I. N. Herstein, *Topics in Algebra*, 2nd ed., John Wiley & Sons, New York, 1975.
4. I. N. Herstein, *Abstract Algebra*, 2nd ed., Macmillan, New York, 1990.
5. F. W. Levi, Notes on group theory. I, II. *J. Indian Math. Soc.* (N.S.), 8 (1944) 1–9.

Department of Mathematics
University of Minnesota, Duluth
Duluth, MN 55812
jgallian@ua.d.umn.edu

Department of Mathematics
University of California, Berkeley
Berkeley, CA 94720
reid@math.berkeley.edu

UNSOLVED PROBLEMS

Edited by: **Richard Guy**

In this department the MONTHLY presents easily stated unsolved problems dealing with notions ordinarily encountered in undergraduate mathematics. Each problem should be accompanied by relevant references (if any are known to the author) and by a brief description of known partial or related results. Typescripts should be sent to Richard Guy, Department of Mathematics & Statistics, The University of Calgary, Alberta, Canada T2N 1N4.

Is There a k-Anisohedral Tile for $k \geq 5$?

John Berglund

Let T be a **monohedral** (all tiles are congruent) tiling of the Euclidean plane [2, p. 20]. Let S(T) be the group of symmetries which map T onto itself. For a given tile T in T let the transitivity class of T be the collection of all tiles to which T can be mapped by one of the symmetries of S(T). If T has precisely k transitivity classes, call T k-**isohedral**. Since a picture is worth 10^3 words, let us look at an example. FIGURE 1 is a tiling that is 1-isohedral. 1-isohedral tilings are also called merely isohedral. FIGURE 2 is a tiling that is 2-isohedral. The shaded tiles form one transitivity class, and the unshaded tiles form another.

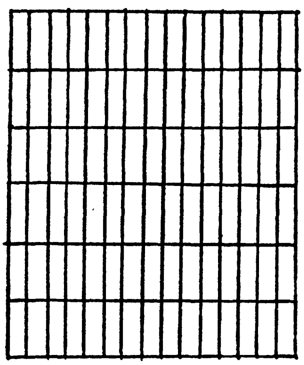


Figure 1. 1-isohedral tiling.

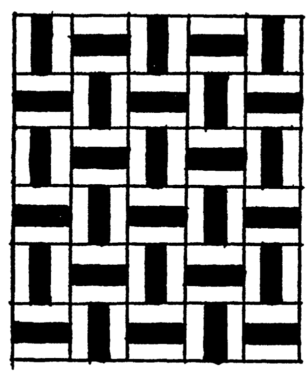


Figure 2. 2-isohedral tiling.

If a tile permits a k-isohedral tiling but not any n-isohedral tiling for $n < k$, call the tile k-**anisohedral**. For example, the tile given in FIGURE 3 is 2-anisohedral. The members of the shaded transitivity class bite the chins of the members of the unshaded transitivity class. The members of the unshaded transitivity class bite the noses. The tile in FIGURE 2 is not 2-anisohedral since it allows the 1-isohedral

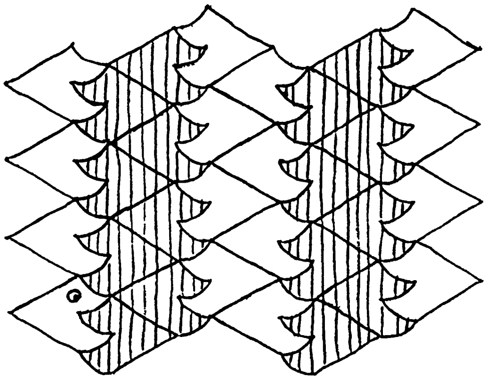


Figure 3. 2-anisohedral tile.

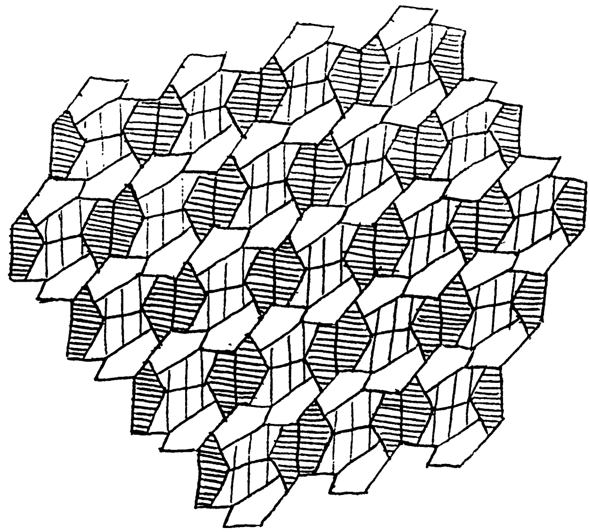


Figure 4. 3-anisohedral tile.

tiling given in FIGURE 1. 3-anisohedral tiles are rarer. As one example, take the Stein pentagon (FIGURE 4) [**2**, p. 518].

4-anisohedral tiles are still rarer. The figure shown in FIGURE 5 seems to be the first published example. Note that the shape is made by joining nine equilateral triangles at the edges.

Problem 1. Do there exist k-anisohedral tiles for every k? Examples have been found for $k \leqslant 4$.

Problem 2. Characterize all k-anisohedral tiles for low values of k. This has been solved for $k = 1$ in Grünbaum and Shephard [**1**]. The general problem has not been solved even for $k = 2$.

To give the reader a taste of these topics, two 4-isohedral tilings are given in FIGURES 6 and 7. Are these shapes 4-anisohedral or not? The shape in FIGURE 6 is

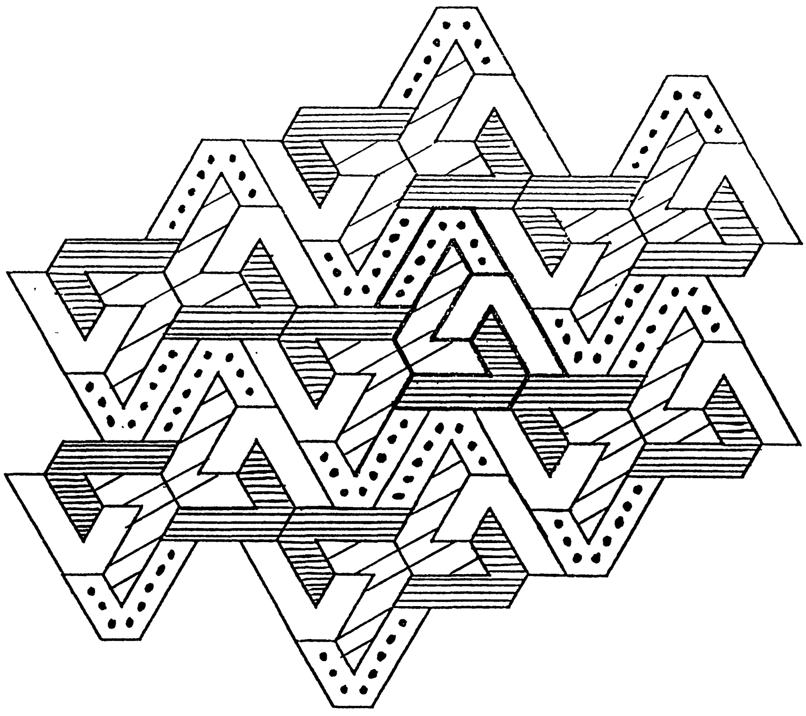


Figure 5. 4-anisohedral polyiamond.

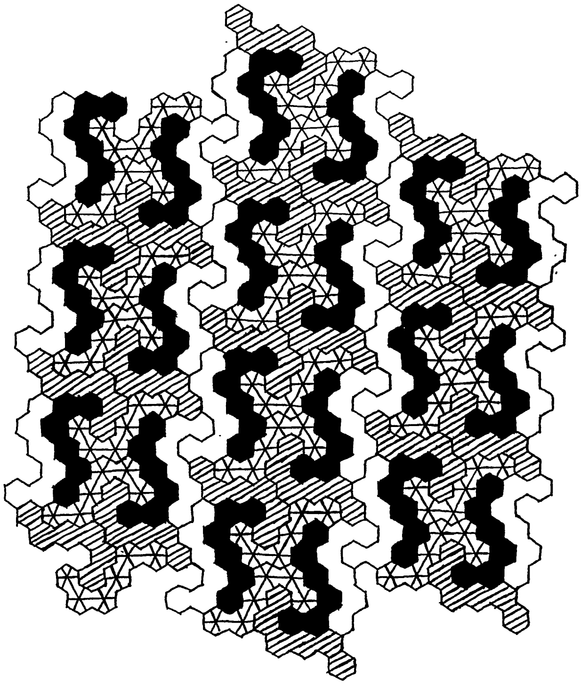


Figure 6. Hexahexe in a 4-isohedral tiling.

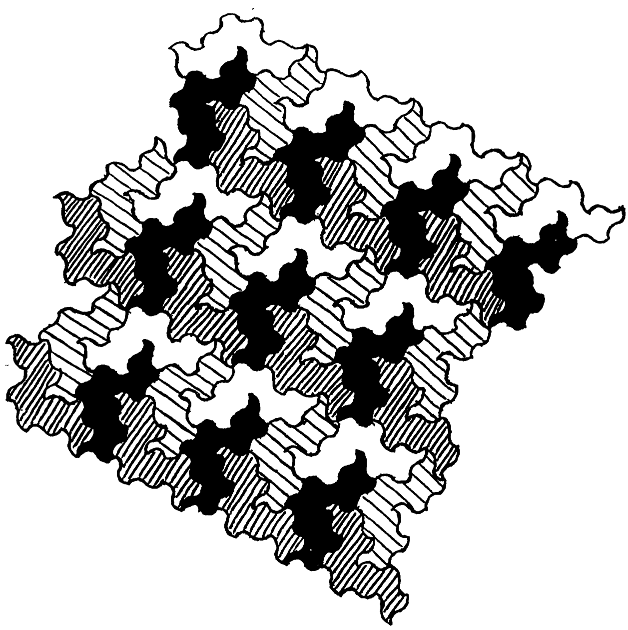


Figure 7. Modified 9-iamond in a 4-isohedral tiling.

made by joining six regular hexagons. The shape in FIGURE 7 is based on a shape made of nine equilateral triangles joined edge to edge; but the edges have been replaced with centrosymmetric curves.

REFERENCES

1. B. Grünbaum and G. C. Shephard, The 81 types of isohedral tilings of the plane. *Math. Proc. Cambridge Philos. Society* 82 (1977), 177–196.
2. B. Grünbaum and G. C. Shephard, *Tilings and Patterns*. Freeman and Co., New York, 1986.

Indiana Academy
Cicero, IN 46034

"... She knew only that if she did or said thus-and-so, men would unerringly respond with the complimentary thus-and-so. It was like a mathematical formula and no more difficult, for mathematics was the one subject that had come easy to Scarlett in her school-days."

From *Gone With the Wind*
by Margaret Mitchell
Submitted by Steven C. Althoen

PROBLEMS AND SOLUTIONS

Edited by:
Richard T. Bumby, Fred Kochman and Douglas B. West

Proposed problems should be sent to the MONTHLY PROBLEMS address given on the inside front cover. Please include solutions, relevant references, etc. Three copies are requested.

Solutions of published problems should arrive before November 30, 1993 at the MONTHLY PROBLEMS address given on the inside front cover. Solutions should be typed with double spacing, including the problem number and the solver's name and mailing address. Two copies suffice. A self-addressed postcard or label should be included if an acknowledgment is desired.

*An asterisk (*) after the number of a problem, or part of a problem, indicates that no solution is currently available. Partial solutions will be useful in such cases. Otherwise, the published solution is likely to be based on a solution which is complete and correct. Of course, an elegant partial solution or a method leading to a more general result is always useful and welcome. In addition, references to other appearances of MONTHLY problems or to solutions of these problems in the literature are also solicited.*

PROBLEMS

10314. *Proposed by Andrew Vince, University of Florida, Gainesville, FL.*

Let b be an integer greater than 1. Let S be a set of integers containing 0 such that no two members of S are congruent modulo b. If

$$\sum_{i=1}^{\infty} \frac{s_i}{b^i} = 0,$$

with $s_i \in S$, prove that all $s_i = 0$.

10315. *Proposed by Mowaffaq Hajja, Yarmouk University, Irbid, Jordan.*

Let A and B be matrices with integer entries of sizes r by n and n by r, respectively, with $r < n$. Suppose that AB is an r by r identity matrix. Show that A can be enlarged to an n by n integral matrix having an integral inverse.

10316. *Proposed by Richard K. Guy, University of Calgary, Calgary, Alberta, Canada, and Richard J. Nowakowski, Dalhousie University, Halifax, N.S., Canada.*

For what pairs of integers a, b does ab exactly divide $a^2 + b^2 + 1$?

10317. *Proposed by Juan Bosco Romero Márquez, Universidad de Valladolid, Valladolid, Spain.*

Let $\triangle ABC$ be inscribed in a circle $\mathscr{C}$ and let A', B', C' be the midpoints of the arcs $\widehat{BC}, \widehat{CA}, \widehat{AB}$, respectively.

(a) Prove that the incenter of $\triangle ABC$ is the orthocenter of $\triangle A'B'C'$.

(b) Prove that the pedal triangle of $\triangle A'B'C'$ is homothetic to $\triangle ABC$

10318. *Proposed by William P. Wardlaw, United States Naval Academy, Annapolis, MD.*

Suppose that A is an n by n matrix with rational entries whose multiplicative order is 15; i.e. $A^{15} = I$, an identity matrix, but $A^k \neq I$ for $0 < k < 15$. For which n can one conclude from this that

$$I + A + A^2 + \cdots + A^{14} = 0?$$

10319. *Proposed by Nick MacKinnon, Winchester College, Winchester, U.K.*

Define

$$S_k(n) = \sum_{r=1}^{n} \sin(r^k).$$

Examination of graphs of $S_k(n)$ as a function of n for $1 < k < 2$ reveals some striking patterns. For example, when $k = 1.4$ the graph divides into clearly defined regions: between $n = 1$ and $n = 36$, one has $-.5 < S_{1.4}(n) < 3$; then the value of the function changes rapidly from $S_{1.4}(36) \approx 2.95$ to $S_{1.4}(49) \approx -5.7$; then one has $-6.2 < S_{1.4}(n) < -1.4$ as n goes from 49 to 225; then there is a rapid increase from $S_{1.4}(225) \approx -6.2$ to $S_{1.4}(257) \approx 15.7$. This pattern persists as far as graphs have been drawn.

(a) As a first step to understanding this phenomenon, determine the locations of the jumps in $S_{1.4}(n)$.

(b) Show that similar behavior may be expected for all k with $1 < k < 2$, with the flat regions being longer for k close to 1 and shorter for k close to 2.

10320. *Proposed by Ignacy I. Kotlarski, Oklahoma State University, Stillwater, OK.*

Under the assumption that f_0, f_1 and f_2 are defined on $[0, \infty)$, Laplace transformable, and not equivalent to zero, solve the integral equation

$$\int_0^{\min(x_1, x_2)} f_0(x) f_1(x_1 - x) f_2(x_2 - x)\, dx = e^{-\max(x_1, x_2)}\left(1 - e^{-\min(x_1, x_2)}\right),$$

with $x_1 \geq 0$ and $x_2 \geq 0$, for the three functions f_0, f_1 and f_2.

10321. *Proposed by Carl Axness, Sandia National Laboratories, Albuquerque, NM, Reinhard Schäfke, University of Essen, Essen, Germany, and David Arterburn, New Mexico Tech., Socorro, NM.*

Let μ be a positive real number. Prove

$$\lim_{x \to 1^+} (\ln x)^{1/\mu} \sum_{i=1}^{\infty} x^{-(2i-1)^\mu} = \frac{\Gamma(1/\mu)}{2\mu}.$$

NOTES

Notes: (10317) The *incenter* of a triangle is the center of its inscribed circle, and the *othocenter* is the point of intersection of its altitudes. The feet of the altitudes of a triangle are the vertices of its *pedal triangle*. **(10319)** See the cover!

SOLUTIONS

Repeated Cyclotomic Factors

E 3442 [1991, 438]. *Proposed by Ray Wylie, Furman University, Greenville, SC.*

Given a sequence $\{b_n\}_{n=0}^{\infty}$ of real numbers such that $b_n = 0$ for n sufficiently large, put $B_s = \sum_{t=0}^{\infty} b_{mt+s}$ $(s = 0, 1, \ldots, m-1)$, and let us say that the sequence $\{b_n\}_{n=0}^{\infty}$ has property P_m, where m is a positive integer, if

$$B_0 = B_1 = \cdots = B_{m-1}.$$

Suppose $a_1, a_2, \ldots, a_r$ are positive integers, not necessarily distinct, and let $C(n)$ be the number of r-tuples $(n_1, n_2, \ldots, n_r)$ of integers such that

$$n = n_1 + n_2 + \cdots + n_r, \qquad 0 \le n_i \le a_i \quad \text{for } i = 1, 2, \ldots, r.$$

Prove that the k sequences

$$\{C(n)\}_{n=0}^{\infty}, \{nC(n)\}_{n=0}^{\infty}, \ldots, \{n^{k-1}C(n)\}_{n=0}^{\infty}$$

all have property P_m if and only if at least k of the integers $a_1, a_2, \ldots, a_r$ are congruent to -1 modulo m.

Solution by O. P. Lossers, Eindhoven University of Technology, Eindhoven, The Netherlands. We consider $m > 1$, and let $\zeta = \exp(2\pi i/m)$. Let $B(x) = \sum_{n=0}^{\infty} b_n x^n$ and $F(x) = \sum_{j=0}^{m-1} B_j x^j$. Observe that $B(\zeta^t) = F(\zeta^t)$ for each $t \in \{1, 2, \ldots, m-1\}$. Therefore, if $\{b_n\}_{n=0}^{\infty}$ has property P_m, then $B(\zeta^t) = 0$ for each $t \in \{1, 2, \ldots, m-1\}$ and $B(x)$ is divisible by $1 + x + \cdots + x^{m-1}$. Furthermore, if $B(\zeta^t) = 0$ for each $t \in \{1, 2, \ldots, m-1\}$, then since $F(x)$ is a polynomial of degree $m-1$, $F(x)$ must be a constant times $1 + x + \cdots + x^{m-1}$ so that $\{b_n\}_{n=0}^{\infty}$ has property P_m.

Observe that the polynomial $C(x) = \sum_{n=0}^{\infty} C(n) x^n$ satisfies

$$C(x) = \prod_{i=1}^{r} (1 + x + \cdots + x^{a_i}).$$

Also, for every integer $t \ge 0$, the polynomial $\sum_{n=0}^{\infty} n^t C(n) x^n$ is a linear combination of the polynomials

$$C(x), xC'(x), x^2C''(x), \ldots, x^t C^{(t)}(x).$$

Hence, if the k given sequences all have property P_m, then the previous paragraph implies that all the polynomials $C(x), C'(x), \dots, C^{(k-1)}(x)$ have at least one factor $1 + x + \cdots + x^{m-1}$ which implies that $C(x)$ is divisible by $(1 + x + \cdots + x^{m-1})^k$. Hence, ζ is a zero of $C(x)$ of multiplicity at least k. Since each factor $1 + x + \cdots + x^{a_i}$ has only simple zeroes, it follows that $a_i + 1$ is a multiple of m for at least k values of i. For the converse, observe that if $a_i + 1$ is a multiple of m for at least k values of i, then $C(x)$ is divisible by $(1 + x + \cdots + x^{m-1})^k$. We can conclude that ζ^t is a root of $\sum_{n=0}^{\infty} n^j C(n) x^n$ for each $j \in \{0, 1, \dots, k-1\}$ and each $t \in \{1, 2, \dots, m-1\}$. The converse now follows from the previous paragraph.

Solved also by D. Callan, R. J. Chapman (United Kingdom), M. Dindos (Slovakia), K. S. Kedlaya (student), N. Komanda, and the National Security Agency Problems Group. One incorrect solution was received.

Hardy's Inequality for Geometric Series

6663 [1991, 559]. *Proposed by Walther Janous, Ursulinengymnasium, Innsbruck, Austria and the editors.*

Show that

$$\sum_{j=1}^{N} \left(\frac{1 + x + x^2 + \cdots + x^{j-1}}{j} \right)^2 < (4 \log 2)(1 + x^2 + x^4 + \cdots + x^{2N-2})$$

for $0 < x < 1$ and all positive integers N; also show that the constant $4 \log 2$ is best possible. (If we drop the factor $\log 2$, we have a special case of Hardy's inequality; see Hardy, Littlewood, and Pólya, *Inequalities*, pp. 239–242.)

Solution by Rolf Richberg, RWTH Aachen, Aachen, Germany. Observing that for $0 < x < 1$ and $N \in \mathbb{N}$

$$\int_x^1 \int_x^1 \frac{1 - (st)^N}{1 - st}\, ds\, dt = \sum_{j=1}^{N} \int_x^1 \int_x^1 (st)^{j-1}\, ds\, dt = \sum_{j=1}^{N} \left(\frac{1 - x^j}{j} \right)^2$$

we may reformulate the assertion as

$$\int_x^1 \int_x^1 \frac{1 - (st)^N}{1 - x^{2N}} \frac{ds\, dt}{1 - st} < (4 \log 2) \frac{1 - x}{1 + x} \qquad (0 < x < 1, N \in \mathbb{N}), \qquad (1)$$

which obviously would follow from

$$\int_x^1 \int_x^1 \frac{ds\, dt}{1 - st} < (4 \log 2) \frac{1 - x}{1 + x} \qquad (0 < x < 1). \qquad (2)$$

In order to prove (2) we consider the double integral:

$$\begin{aligned} \int_x^1 \int_x^1 \frac{ds\, dt}{1 - st} &= \int_x^1 \left[-\frac{1}{t} \log(1 - st) \right]_{s=x}^{s=1} dt \\ &= -\int_x^1 \log(1 - t) \frac{dt}{t} + \int_{x^2}^{x} \log(1 - t) \frac{dt}{t} \\ &= -2 \int_x^1 \log(1 - t) \frac{dt}{t} + \int_{x^2}^{1} \log(1 - t) \frac{dt}{t}. \end{aligned}$$

Substituting $t = \tau^2$ in the last integral and noting $\log(1 - \tau^2) = \log(1 - \tau) + \log(1 + \tau)$, we obtain

$$\int_x^1 \int_x^2 \frac{ds\,dt}{1 - st} = 2\int_x^1 \log(1 + t)\frac{dt}{t},$$

thus transforming (2) into

$$\int_x^1 \log(1 + t)\frac{dt}{t} < (2\log 2)\frac{1 - x}{1 + x} \qquad (0 < x < 1). \tag{3}$$

Now, differentiating with respect to t shows that $(1/t)\log(1 + t)$ is a decreasing and $(1 + (1/t))\log(1 + t)$ an increasing function of $t \in (0,1)$. For $0 < x < 1$ we therefore have

$$\begin{aligned}\int_x^1 \log(1 + t)\frac{dt}{t} &< (1 - x)\frac{\log(1 + x)}{x} \\ &= \frac{1 - x}{1 + x}\left(1 + \frac{1}{x}\right)\log(1 + x) < \frac{1 - x}{1 + x}2\log 2,\end{aligned}$$

which proves (3).

Suppose (1) is valid with $4\log 2$ replaced with a constant c. Taking the limit for $N \to \infty$ we then get

$$2\int_x^1 \log(1 + t)\frac{dt}{t} = \int_x^1 \int_x^1 \frac{ds\,dt}{1 - st} \le c\frac{1 - x}{1 + x} \qquad (0 < x < 1).$$

In

$$\frac{2}{1 - x}\int_x^1 \log(1 + t)\frac{dt}{t} \le \frac{c}{1 + x}$$

(which comes from the transformation used to obtain (3)) let x tend to 1. It follows that $2\log 2 \le c/2$, i.e., $c \ge 4\log 2$. Thus, the constant $4\log 2$ is best possible.

Solved also by H. Morris.

An Extremal Set Problem

E3459 [1991, 754]. *Proposed by Constantin Adrian, Timisoara, Romania.*

Suppose X is an n-element set, $n \ge 12$, and suppose F is a family of 4-element subsets of X such that the intersection of each pair of distinct sets in F has at most two elements. Prove that there is a subset S of X containing at least $(6n - 6)^{1/3}$ elements such that none of the 4-element subsets of S is in the family F.

Solution by Fred Galvin, University of Kansas, Lawrence, KS. Call a subset of X *independent* if it contains no member of F. Assuming $n \ge 3$, we show that every maximal independent subset of X has size greater than $(6n)^{1/3}$.

Let S be a maximal independent set, with $k = |S|$. Clearly $k \ge 3$. Since S is maximal, for each $x \in X - S$ there is a 3-element set $f(x) \subseteq S$ such that $f(x) \cup \{x\} \in F$. The condition on F implies that f is injective. Hence $n - k \le \binom{k}{3}$, or $6n \le 6\binom{k}{3} + 6k = k^3 - 3k^2 + 8k \le k^3 - 3$, and so $k \ge (6n + 3)^{1/3}$.

Editorial comment. Solvers proved various inequalities of the form $k \ge (6n + c)^{1/3}$ for $n \ge n_0$; by choosing n_0 large enough, c can be made arbitrarily large.

Fred Galvin noted that this problem is a special case of a class of problems discussed (but not explicitly solved) by Paul Erdős in "Problems and results on graphs and hypergraphs: similarities and differences," in *Mathematics of Ramsey Theory* (J. Nesetril and V. Rödl, eds.), Springer-Verlag, 1990, 12–28. The function $h_r(n, p, q)$ is the maximum integer m such that if each r-element subset of an n-set X is colored red or blue, then there exists a p-element subset of X containing at least q red r-sets or an m-element subset of X whose r-sets are all blue. The statement of this problem is $h_4(n, 5, 2) \geq (6n - 6)^{1/3}$ for $n \geq 12$.

Solved also by G. Calinescu (student, Romania), R. J. Chapman (U. K.), J. R. Griggs, R. Jeurissen (the Netherlands), I. Kastanas, O. P. Lossers (The Netherlands), B. Peterson, P. Tracy, and the proposer.

Source-Even Orientations of Graphs

E 3462 [1991, 755]. *Proposed by J. J. Rotman, University of Illinois at Urbana, Champaign, IL.*

Prove that any connected simple graph with an even number of edges has an orientation (assignment of direction to each edge) such that the number of edges leaving each vertex is even.

Solution I by Richard Holzsager, The American University, Washington, DC. Suppose the edges of the graph are oriented to minimize the number of vertices that are sources of an odd number of edges. Since the total number of edges is even, there must be an even number of such vertices. If this even number is positive, find a path connecting two of these vertices (guaranteed by the graph being connected) and reverse the orientation of each edge in the path. This does not change the parity of edges leaving any intermediate vertex along the path, but it changes the endpoints from odd to even, contradicting minimality.

Solution II by Jerrold Grossman, Oakland University, Rochester, MI. It is well-known that every connected graph with an even number of edges can be decomposed into edge-disjoint copies of P_3, the path containing two edges. (See, for example, exercise 8.21a in G. Chartrand and L. Lesniak, *Graphs and Digraphs* (Second edition), Wadsworth, 1986.) Given such a decomposition, we orient the edges of each P_3 from its center toward its endpoints. This orientation has an even number of edges leaving every vertex.

Editorial comment. (1) Many solvers noted that simplicity of the graph is not necessary; neither of the above proofs requires this assumption. (2) Many solvers also mentioned the following easy extension to connected graphs with an odd number of edges: For any vertex v in such a graph, there is an orientation such that the number of edges leaving v is odd and the number of edges leaving every other vertex is even. (3) F. Galvin, J. Conklin, and E. Stone proved that the number of orientations having the desired property is exactly 2^{m-n+1}, where m is the number of edges and n is the number of vertices. (4) F. Galvin offered an extension to infinite graphs: Let G be an infinite graph and let V_F be the set of vertices of finite degree. Then, for any mapping p: $V_F \to \{0, 1\}$, there is an orientation of G such that, for every vertex $v \in V_F$, the number of edges leaving v has the same parity as $p(v)$.

Solved also by 46 others and the proposer.

A Permutation on the Cube

6670 [1991, 862]. *Proposed by R. H. Jeurissen, Toernooiveld, Nijmegen, The Netherlands.*

Let $\{0,1\}^n$ denote the set of n-bit strings of zeros and ones. If $(a_1,\dots,a_n) \in \{0,1\}^n$, let $\pi_n(a_1,\dots,a_n)$ be the string $(b_1,\dots,b_n)$ given by $b_1 = a_1$ and $b_k \equiv a_k + a_{k-1} \pmod 2$ for $1 < k \le n$. Since $(a_1,\dots,a_n)$ can be retrieved from $(b_1,\dots,b_n)$, it is clear that π_n is a permutation of $\{0,1\}^n$. Determine the cycle structure of the permutation π_n, i.e., the lengths of the cycles that occur and the number of cycles of each length.

Solution by Thomas Honold, Technische Universität München, München, Germany and Sonja Maus, Bonn, Germany (independently). The cycle lengths are powers of 2. If c_k denotes the number of cycles of length 2^k, then

$$c_k = \begin{cases} 2 & \text{if } k = 0 \\ 2^{-k}\left(2^{2^k} - 2^{2^{k-1}}\right) & \text{if } 2 \le 2^k \le n \\ 2^{-k}\left(2^n - 2^{2^{k-1}}\right) & \text{if } n \le 2^k \le 2n \\ 0 & \text{if } 2^k \ge 2n \end{cases}$$

To establish this result, identify $\{0,1\}^n$ with the vector space V of n-tuples over $GF(2)$, the field with two elements. Then π_n is an automorphism of V, and $\pi_n = I + N$, where I is the identity operator and N is the shift operator defined by $N(a_1,\dots,a_n) = (0, a_1,\dots,a_{n-1})$. Note that N is nilpotent, with $N^n = 0$. Since we are working over $GF(2)$, we have $\pi_n^{2^k} = I + N^{2^k}$ for every integer positive k. It follows that the order of π_n is a power of 2 and hence so is the length of every cycle of π_n. Now $v \in V$ is fixed by π_n if and only if $v \in \ker(N)$, and v lies in a cycle of length 2^k with $k \ge 1$ if and only if $v \in \ker(N^{2^k}) - \ker(N^{2^{k-1}})$. The result now follows from the observation that $\dim(\ker(N^j)) = \min\{n, j\}$.

Editorial comment. J. C. Binz and Tad White (independently) extended the result to the analogous automorphism of the vector space of n-tuples over $GF(p)$ for any prime p. Arthur Woerheide extended it even further to the analogous automorphism of G^n where G is any finite-dimensional vector space over $GF(p)$. These extensions are easily derived by appropriate modifications to the given solution.

Solved by 30 solvers (including those cited) and the proposer.

Deferred Cesàro Means

10217 [1992, 362]. *Proposed by Brian Philp, The University of Birmingham, Birmingham, England.*

Suppose $\{\alpha_j\}_{j=1}^{\infty}$ is a sequence of complex numbers.
(a) Prove that if $n^{-1}\sum_{j=n}^{2n}\alpha_j \to \lambda$ and $n^{-1}\sum_{j=n}^{4n}\alpha_j \to 3\lambda$, then $n^{-1}\alpha_n \to 0$.
(b) Is it true that if $n^{-1}\sum_{j=n}^{3n}\alpha_j \to 2\lambda$ and $n^{-1}\sum_{j=n}^{9n}\alpha_j \to 8\lambda$, then $n^{-1}\alpha_n \to 0$?

Solution by Robin J. Chapman, University of Exeter, Exeter, U. K.
(a) By replacing α_n by $\alpha_n + \lambda$ we may, and shall, assume that $\lambda = 0$. Let $\beta_n = n^{-1}\alpha_n$. Now

$$\frac{\alpha_{2n}}{n} = \frac{1}{n}\sum_{j=n}^{2n}\alpha_j + \frac{2}{2n}\sum_{j=2n}^{4n}\alpha_j - \frac{1}{n}\sum_{j=n}^{4n}\alpha_j$$

and so $\beta_{2n} \to 0$ as $n \to \infty$. It follows that $\delta_n = n^{-1}\Sigma_{j=n}^{2n-1}\alpha_n \to 0$ as $n \to \infty$. Now $(n+1)\delta_{n+1} - n\delta_n = \alpha_{2n+1} + \alpha_{2n} - \alpha_n$ and so

$$\begin{aligned}\beta_{2n+1} &= \frac{n+1}{2n+1}\delta_{n+1} - \frac{n}{2n+1}\delta_n - \frac{2n}{2n+1}\beta_{2n} + \frac{n}{2n+1}\beta_n \\ &= \gamma_n + \frac{n}{2n+1}\beta_n\end{aligned}$$

where $\gamma_n \to 0$ as $n \to \infty$. Hence $|\beta_{2n+1}| \le |\gamma_n| + |\beta_n|/2$. Given $\varepsilon > 0$ choose N such that $|\gamma_n|, |\beta_{2n}| < \varepsilon$ if $n \ge N$. Let $K = \max(|\beta_N|, |\beta_{N+1}|, \dots, |\beta_{2N}|)$. I claim that if $2N \le m \le 4N$ then $|\beta_m| \le \varepsilon + K/2$. This is trivial if m is even and if $m = 2n+1$ is odd then $|\beta_m| \le |\gamma_n| + |\beta_n|/2 \le \varepsilon + K/2$ as required. If we define $f_\varepsilon(K) = \varepsilon + K/2$ then iterating this argument gives $|\beta_m| \le f_\varepsilon^r(K)$ (the r-fold iterate of f_ε applied to K) for $2^rN \le m \le 2^{r+1}N$. Now for fixed ε and large r, $f_\varepsilon^r(K) \to 2\varepsilon$ and hence $|\beta_m| \le 3\varepsilon$, as required.

(b) The answer is "no." I claim we can choose the α_{3k+1} for $k \ge 0$, arbitrarily so that $\Sigma_{j=n}^{3n}\alpha_j = \Sigma_{j=n}^{9n}\alpha_j = 0$. We make $\alpha_{3k} = 0$ for all $k \ge 1$ and if $k \ge 0$ define α_{3k+2} for $k \ge 0$, recursively by $\alpha_{3k+2} = -\Sigma_{j=k+1}^{3k+1}\alpha_j$. It is now clear that $\Sigma_{j=n}^{3n}\alpha_j = \Sigma_{j=n}^{9n}\alpha_j = 0$. But choosing say $\alpha_{3k+1} = k^2$ we can make $\{n^{-1}\alpha_n\}_{n=1}^{\infty}$ unbounded.

Editorial comment. The problem arose in connection with noticing that the claimed necessary and sufficient condition

$$\frac{1}{n}\sum_{j=n}^{\lambda n}\alpha_j \to (\lambda - 1)s \quad \text{as } n \to \infty \text{ for some } \lambda > 1$$

for Cesàro summability given as "analytic background" in Theorem IV of N. H. Bingham, "On Tauberian theorems in probability theory", *Nieuw Arch. Wisk.* (4) 3 (1985), 157–166 was incorrect. Part (b) provides a counterexample to this statement. In general, a second value of $\lambda \ge 1$ is needed. A proof of the positive result given in part (a) due to Prof. B. Kuttner was provided by the proposer.

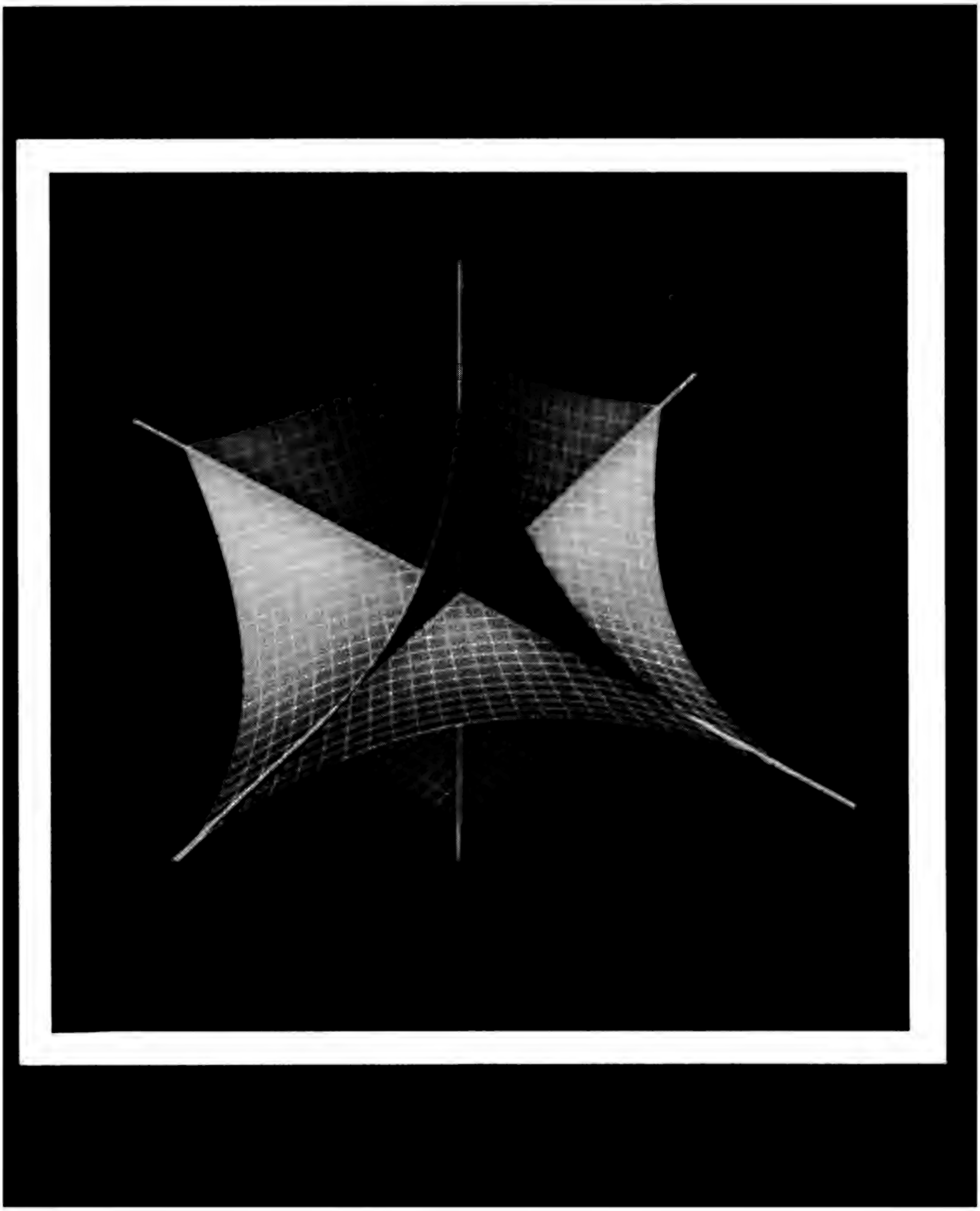
Solved also by M. Dindos (Slovakia), N. J. Fine, K. S. Kedlaya (student), O. P. Lossers (The Netherlands), M. Mócsy (Hungary), and R. Stong. One solution dealing only with part b, one for which only part b was correct, and one incorrect solution were also received.

Answer to Picture Puzzle:
(p. 538)

John Littlewood, sometimes described as the name Hardy invented for a collaborator.

The American Mathematical Monthly

Volume 100, Number 7 / AUGUST–SEPTEMBER 1993



NOTICE TO AUTHORS

The *Monthly* publishes articles, notes, and other features about mathematics and the profession. The readership of the *Monthly* is intended to include everybody who is mathematically inclined, including of course professional mathematicians and students of mathematics at all collegiate levels. While no single article or feature is likely to appeal to everyone, material should interest and be accessible to a large number of readers. This is the most important criterion for acceptance.

Articles may be expositions of old results or presentations of new ones. They may concern all of mathematics or one small area, a broad development or a single application, historical reminiscences or one important event. While some articles may contain the author's new research, the novelty of material and generality of the results is far less important than the clarity of exposition and general interest. Discussing one illuminating case of a well known result is far better than providing all the details of an obscure but new proposition. Articles in the *Monthly* are supposed to inform and to entertain; they are meant to be read rather than archived.

Notes are short and possibly informal articles. A note may concern a clever new proof of an old theorem, a novel way to present tired material, or a lively discussion of a philosophical (but still mathematical) issue. Also, any topic is suitable, so long as it is related to mathematics. Because a note is short, the first few sentences are the most important part: They should explain the purpose and invite the reader in. Photographs or diagrams often will attract the reader's attention.

All articles and notes should be sent to the editor:

JOHN EWING,
Department of Mathematics,
Indiana University,
Bloomington, IN 47405.

Please send 3 copies, typewritten on only one side of the paper. Illustrations should be carefully drawn on separate sheets of paper in black ink; the original should be without lettering and two copies should have appropriate captions and lettering indicated.

Proposed problems or solutions should be sent to:

RICHARD BUMBY,
P.O. Box 10971
New Brunswick, NJ 08906-0971.

Please send 2 copies of all material, typewritten if possible.

Letters to the Editor, both for publication and for private reading, should be sent to the Editor at the address given above. Comments, including criticisms, are welcome, as are all suggestions for making the *Monthly* a lively, entertaining, and informative journal.

Reprint permission:
MARCIA P. SWARD, Executive Director

Advertising Correspondence:
Ms. ELAINE PEDREIRA, Advertising Manager

Subscription correspondence, change of address, and other inquiries:
Membership / Subscriptions Department

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036.

Microfilm Editions: University Microfilms International, Serial Bid coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

The AMERICAN MATHEMATICAL MONTHLY (ISSN 0002-9890) is published monthly except bimonthly June-July and August-September by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, DC 20036 and Montpelier, VT.

Second class postage paid at Washington, DC, and additional mailing offices. ***Postmaster***: Send address changes to the American Mathematical Monthly, Membership / Subscription Department, MAA, 1529 Eighteenth Street, N.W., Washington, DC, 20036-1385.

The American
Mathematical Monthly

Volume 100 Number 7 / AUGUST-SEPTEMBER 1993
(ISSN 0002-9890)

Contents

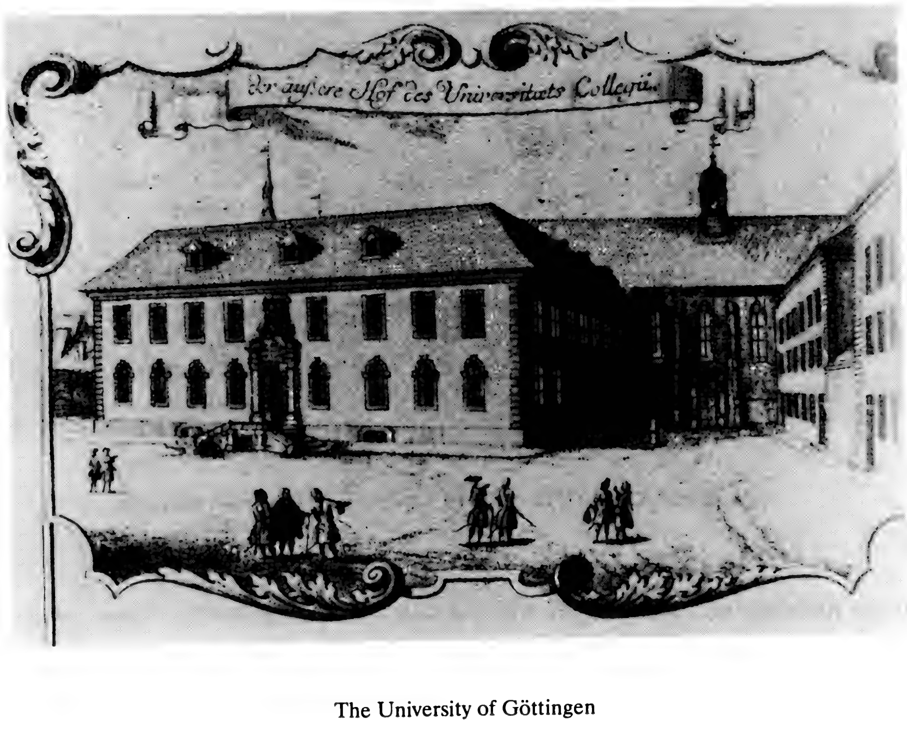
ARTICLES

FEATURES

Thomas Archer Hirst—
Mathematician Xtravagant
III. Göttingen and Berlin

J. Helen Gardner and Robin J. Wilson

I carry with me all manner of letters of introduction to Göttingen, but the making of new acquaintances is ever a task to me; and for my own part I would rather have dispensed with extraneous help in doing so. It is a worse thing to be over- than under-estimated, and there is ever far more satisfaction in silently carving one's own path than in having it made ready and carpeted for us...

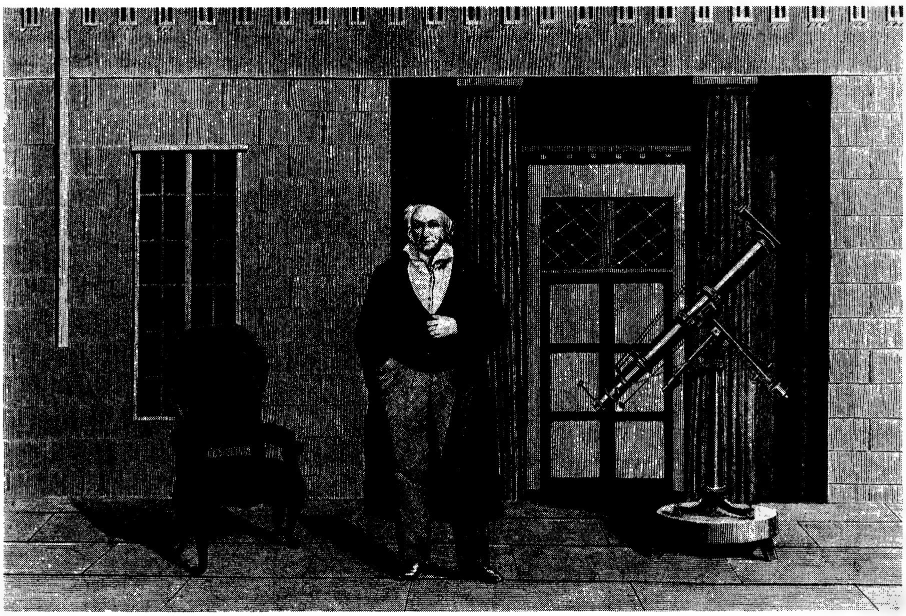


The University of Göttingen

With the completion of his Ph.D. thesis in Marburg, Thomas Hirst decided to travel, making Göttingen his first port of call. Here he spent two weeks at the University, attending lectures and conducting magnetic experiments with the physicist Wilhelm Weber, 'a curious little fellow [who] speaks in a shrill, unpleasant and hesitating voice'. He also attended Moritz Stern's 'beautifully clear' lectures on integral calculus and mechanics, and was much impressed by him.

6th August 1852: To-day I called on Weber again. He received me kindly and explained to me a new method of his of determining the inclination of the Magnet. He speaks and stutters on unceasingly; one has nothing to do but to listen. Sometimes he laughs for no earthly reason, and one feels sorry at not being able to join him. At 2 p.m. I went with him to make some experiments—he, I and another student made a determination of the Magnetic Inclination. I read off the "Auschlags Winkel" [angle of inclination] and though my first attempt, we got a result of 67° 26′—that is within the daily variation...

Stern is a stern fellow, a firm, rub-against-able fellow—not an atom of unnecessary ceremony about him, but the greatest plainness and character. We got a bit of brown bread and butter together, as he would have taken himself, with a glass of water to it, and then a cigar. At first we talked about a dark point in his lecture, then on a multitude of topics. Stern is a widower with a family, a housekeeper; I believe his wife destroyed herself. At any rate, she went insane and either killed herself or died. It is said that for long after he was a misanthrope—one can see several deep wrinkles of sorrow in his face, though his manner is now gentle and quiet...



Carl Friedrich Gauss (1777–1855) on the terrace of Göttingen University

But the highlight of his Göttingen trip was a visit to Carl Friedrich Gauss, which he recorded in great detail.

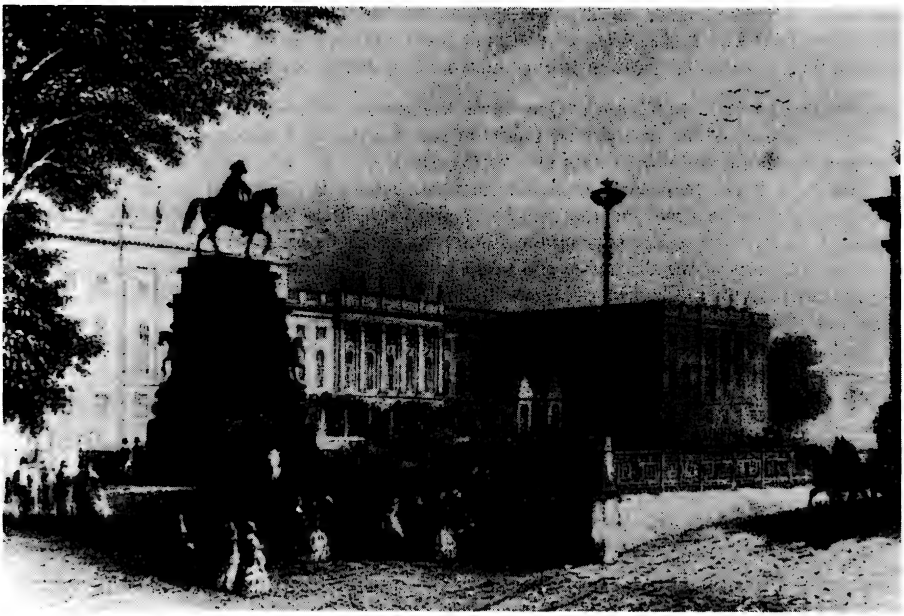
12th August 1852: ...Personally he is a venerable, fine old fellow, with a contented manly expression. There is an extraordinary aspect of power about him and his every word: without effort he suggests to every one the presence of manly might. He is about 80 years of age, but not a trace of superannuation is to be seen about him. He can even read without spectacles. Although our interview as far as the conversation was concerned was not brilliant or extraordinary, for in it there was no effort on either side, yet for remembrance sake I will try to relate it. No sooner was the first word spoken than I felt perfectly at ease, and he pointed for me to sit on the sofa and took a chair close by me. We spoke of course all in German, though he can speak English.

Tom. I am sorry, Professor, that I have not had the opportunity of hearing a lecture from you during my stay in Göttingen. It was, in fact, one of my principal motives for coming—a kind of

curiosity perhaps it may be called, yet for a lover of science I hope at least an excusable one.
Gauss. Ah, this semester few students announced themselves, and at my age, with other work to be yet finished by me, and the hot summer before me, I was glad rather than otherwise to be dispensed from the task.
Tom (after a short silence). Have you ever been in England, Professor?
Gauss. No, I never got further than Belgium, and now the difficulties of the journey, as well as the change of life and habits render it impossible for me.
Tom. It is true this difference in habits and life affect even younger and stronger persons. I suffered somewhat myself from the same cause.
Gauss. Yet, considering the great esteem I have for the English as a nation, which we may consider a model for us as far as steady, persevering toil and firmness of character are concerned, it is now strange to me that in my younger days I never visited it.
Tom. You have, however, the consolation to know that it was your own work that prevented you. Yet there is something about your German life (especially student life) that so far excels English as yearly to draw more and more of us to your universities...

So we chatted on quite comfortably for three-quarters of an hour, and then I bid the old veteran good-bye and thanked him heartily. I left him copies of some of Tyndall's memoirs and of my own dissertation.

As a mathematician, Gauss is without doubt our Sir Isaac Newton. Perhaps no one ever had a firmer reliance in the absolute truth of mathematics, or lived more in it. It is to him the foundation of the universe on which God himself has built...



The University of Berlin, now known as Humboldt University

After leaving Göttingen, Hirst spent several weeks travelling around Germany and Austria with his brother John and some friends from Marburg. He then moved to Berlin, where he spent the winter semester, from October to April. On his arrival, he went to visit the algebraist Ferdinand Eisenstein, 'a young and highly promising mathematician'. Unfortunately, Eisenstein had died just the day before. This, understandably, upset Hirst considerably.

12th October 1852 ... A young, able fellow, cut down the moment he was making his ability known and useful—a fellow of deep intellect and great industry, too, as late journals can show. We entered joyfully, thinking to see him and know him; we left it awe-struck, silent and sad.

The next morning he called on Lejeune Dirichlet, the distinguished analyst and number theorist, and 'met with a very hearty reception'.

13th October 1852: He is a rather tall, lanky-looking man, with moustache and beard about to turn grey (perhaps 45 years old), with a somewhat harsh voice and rather deaf: it was early, he was unwashed, and unshaved (what of him required shaving), with his "schlafrock", slippers, cup of coffee and cigar... I thought, as we sat each at an end of the sofa, and the smoke of our cigars carried question and answer to and fro, and intermingled in graceful curves before it rose to the ceiling and mixed with the common atmospheric air, "If all be well, we will smoke our friendly cigar together many a time yet, good-natured Lejeune Dirichlet."

Although he continued to read widely in all branches of mathematics, he increasingly felt the need to further his knowledge of geometry. He was particularly interested in the relationship between synthesis and analysis.

15th October 1852: After having purchased three valuable volumes, Carnot's "Geometrie de Position", Gauss's "Theory of Numbers" (in French) and Cauchy's application of Diff: Cal: to Geometry, I find my hands full of work. My own books have also arrived from Marburg; how dependent one is on books. I felt lost without them, and had to ask myself: "Tom, hast thou nothing then in thee, but must be strung and wound up before thou canst begin playing?'...

18th October 1852: ... In Carnot's "Geometrie de Position" with which I am now engaged, after an able discussion of the comparative merits of and distinctions between so-called analysis and synthesis occurs the following rather noteworthy paragraph:

"Synthesis is not exclusively applied to mathematics—it is in general the art of reasoning with justice: whatever may be the subject of argument. It is identical with what is termed dialectics... Analysis proceeds generally differently, in that series of transformations are made on truncated parts of the discourse, and taken isolately are unintelligible, but which submitted like the others to the mechanism of argumentation can by a new series of transformations lead to clear and precise results—as much so, indeed, as those deduced synthetically..."

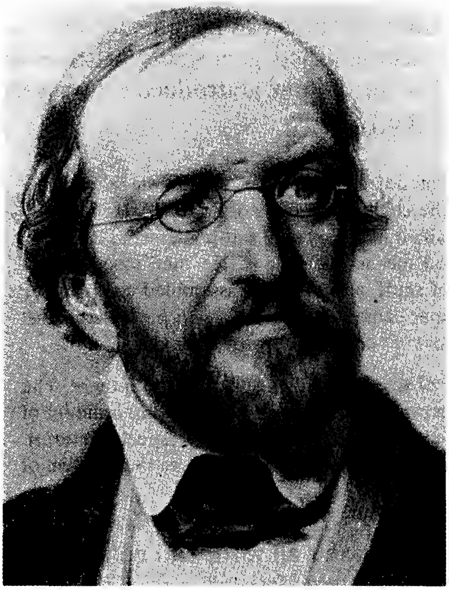
... Carlyle tells me that just at this time he [Carnot] was taking his part in the French Revolution—who knows but he may have written it after that memorable dinner party at which he and Robespierre were with others present, when Carnot slipped out of the room, searched Robespierre's pocket that he had laid aside, and found therein a sentence of death for himself and others with whom that Robespierre had been chatting quite coolly...

It was not long before the lectures began. Hirst was particularly impressed by those of Jakob Steiner, both for his pure synthetic approach to geometry (which accorded with Hirst's own views) and also for his attitudes to education, which he acquired while studying at the school of the Swiss reformer Pestalozzi.

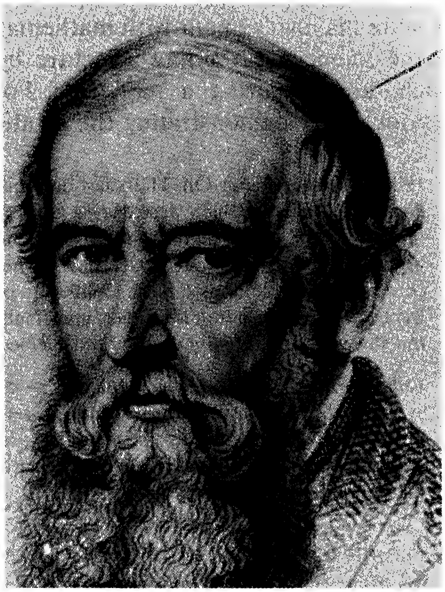
28th October 1852: ... I have heard Steiner twice, and am well pleased with him. He is a middle-aged man, of pretty stout proportions, has a long, intellectual face, with beard and moustache, and a fine prominent forehead, hair dark and rather inclining to turn grey. The first thing that strikes you on his face is a dash of care and anxiety almost pain, as if arising from physical suffering. Before starting he sets his chair right, looks all round, finds the window must be opened, and with difficulty gets started. Then in a short time he will ask them to close the window within a hand's breadth, for he has rheumatism. All these point to physical nervous weakness. His Geometry is famed for its ingenuity and simplicity—he is an immediate pupil of Pestalozzi: in his youth was a poor shepherd boy, and now a professor. His argument is that the simplest way is the best; he tries ever to find out the way Nature herself adopts (not always, however, to be relied upon). Mathematics he defines to be the "Science of what is self-evident"...

But most of all, he admired the teaching of Dirichlet:

31st October 1852: Dirichlet cannot be surpassed for richness of material and clear insight into it: as a speaker he has no advantages—there is nothing like fluency about him, and yet a clear eye and understanding make it dispensable: without an effort you would not notice his hesitating speech. What is peculiar in him, he never sees his audience—when he does not use the black-board at which time his back is turned to us, he sits at the high desk facing us, puts his spectacles up on his forehead, leans his head on both hands, and keeps his eyes, when not covered with his hands, mostly shut. He uses no notes, inside his hands he sees an imaginary calculation, and reads it out to us—that we understand it as well as if we too saw it. I like that kind of lecturing.



Lejeune Dirichlet (1805–1859)



Jakob Steiner (1796–1863)

While enjoying the lectures of Steiner and Dirichlet, he was also developing their friendship. His social calls became increasingly frequent, and his diary entries around this time seem to alternate between the two. However, the two men could not have been more different, and this difference shines out of the words—the grumpy and ailing Steiner, with 'a power of insight possessed by no other living geometer, perhaps', and the genial Dirichlet, with whom he was becoming 'on terms of perfect friendship'. But, for all this, he seems to have been fond of both of them, and any adverse comments were statements of fact, as he saw it, rather than condemnations.

7th November 1852: ...To-day I called on Prof. Riess of the "Königliche Academie der Wissenschaft"... Riess is a delicate, good man, with clear, deep insight. I listened with great interest to his talk about Dirichlet, Jacobi and Steiner. He told me fully the relations on which the latter stands with them all, and truly it is unexplainable. Riess says his vulgarity has by them all been slightly borne in consideration of his undoubted genius. But that some time ago without provocation Steiner cut them all. The probable reason is that Steiner, naturally of a testy disposition, which has been increased, too, by bodily illness, feels himself slighted that he has been 33 years "Ausserordentliche" [Extraordinary] Professor. The reason is clear: firstly he does

not know Latin, and that among German professors is held as a necessity: 2nd he is so terribly one-sided on the question of Synthetical Geometry that as an examiner he would not be liked. The more I hear, the more I am determined to see him and study him for myself.

14th November 1852: ...Wednesday evening I spent with Dirichlet: saw Mrs Dirichlet again, found she was sister to Mendelssohn—she played me several of her brother's pieces, to which I listened with great willingness.

21st November 1852: On Tuesday I called again to see Steiner. He came to me first in his ante-room, when we had a little interesting talk on his system of Synthetical Geometry, and its relation to Analysis. The latter he would by no means annihilate, and pleads justly that heretofore it has but had too great pre-eminence to the detriment of Synthesis. I mentioned that I had in view to translate his work into English—the old fellow's indifference towards me has been somewhat relaxing before, and this was the finishing stroke...

Despite his involvement with mathematics, Hirst continued to keep us his interests in the sciences, attending a lecture by the distinguished geologist Christian von Buch, and admiring a model of Foucault's pendulum, introduced two years previously for demonstrating the rotation of the Earth.

19th December 1852: On Thursday du Bois [Reymond] came to take me to the Königliche Academie. Old von Buch was reading a paper on the chalk formations of America. He is also a fine old fellow, with a stern iron face... Steiner walked in with a very self-possessed, glum face, which relaxed into a smile and a bow as he passed me near the door. He then stood at one corner of the table, took a large, deliberate pinch of snuff, and eyed the assembled company... Buch was sitting reading his paper, and finally Steiner came to a standstill with his back against the stove, took snuff very largely, and seemed to have no connection with anybody.

13th February 1853: Monday at Magnus's—a party of scientific ladies and gentlemen there. The evening was spent by Magnus shewing us several experiments. Magnus was shewing a model of Foucault's experiment with the pendulum; as he said, for Dirichlet's and my especial interest. The only remark the ladies made on the matter (and they always make some) was that motion of the pendulum was "sehr gracieuse."

His studies took most of his waking hours, but it wasn't all work and no play. Hirst took advantage of the crisp winter weather to pursue a 'favourite amusement'.

20th February 1853: This has been a winter's week indeed—10° below Zero in Baumer. Cabs has been almost entirely replaced by sledges, and the streets are in a continual tinkle, tinkle. I have for the first time in my life had a ride in one, on Wednesday, and very easy riding I found it. On Wednesday, and this afternoon, I had some skating for the first time in Germany—indeed, for many years. Swimming in summer and skating in winter are the two greatest physical enjoyments I indulge in, and I have a weakness for both. The scene on the ice here in the Thiergarten is novel and attractive to me. There are ladies by the score skating beautifully... Prof. Mitscherlich's daughter was skating gracefully past me, and I, rogue that I am, was looking at her skates (and the ankles to which they were fastened) instead of my own, and I suffered for it. With a fearful crash I came on my rump. I did not break the ice, but I certainly left "my mark" there in the shape of an asterisk...

But more often than not, Hirst was working hard, involved both with his mathematics, and also with his teachers—in particular, Dirichlet and Steiner. There are comments on their teaching styles, as well as frequent references to their personalities and activities.

20th February 1853: ...I will here record a few peculiarities in Steiner's lectures. He never prepares them beforehand, but follows ideas as they suggest themselves. He thus often stumbles or fails to prove what he wishes at the moment, and at every such failure he is sure to make some characteristic remark... Dirichlet has also his peculiarities—one is of forgetting time; he pulls his watch out, finds it past three, and runs out *without even finishing the sentence.*

3rd April 1853: ... Steiner remains working at home until nearly 4 p.m.; he then dines at Schultz's Wein Keller—after dinner he takes a long walk until 6 or 7, returns home, works or sleeps until 11:30 or 12, and then comes to Schultz's again to drink a glass of grog and eat his supper. Here he shows his testiness most—the waiter he rated soundly for not bringing him his usual sort of wine—a person interrupted him whilst speaking, and got from him a stormy reprimand. After 1 a.m. we accompanied him home... Yesterday after dining again with Knoblauch, I was walking down the Linden and heard an unmistakeable voice (viz. Steiner's) calling my name. I turned with him, and we had a short walk. We spoke much on the old question of the relative claims of Analysis and Synthesis in Geometry, and I found him more liberal than ever before. As we returned, I asked if for once he would step into my lodgings and sit half an hour with me. He did so. And thus for once he paid a visit—a thing he seldom or never does...

24th April 1853: Wednesday evening we spent with Dirichlet... During the evening Prof. Hensel (husband to the late Fanny Hensel, another sister of Mendelssohn's) came. It was proposed that we should make the experiment of moving the table (Tisch rücken) which is now the subject of fashionable twaddle. Hensel had seen it the evening before and believed in it thoroughly. I and Dirichlet were thoroughly sceptical, Mrs D. was indifferent, and Dickinson and another gentleman were inclined to be believers. We sat for half an hour, each one placing both hands on the table and placing the little finger of his right hand on the little finger of his neighbour's left hand. The table was a pretty stout round one, with one leg rolling on three pulleys. It was easily movable by a single person. The experiment was totally unsuccessful... I believe the table would have moved this evening had we all been in a sufficient unanimity; one thought the table was leaning a little in one direction; directly two or three more are intent upon it so moving—look anxiously in that direction,—and unconsciously help it. The scientific men in Berlin almost all ridicule the idea. It deserves, however, a closer experiment.

Shortly afterwards, Hirst left Berlin for two months in Paris, where he attended the mathematics lectures of Joseph Liouville and Gabriel Lamé, before returning to England to take up a schoolteaching appointment at Queenwood College, in Hampshire. His time at Queenwood, his marriage, and his subsequent return to France, will be described in the next article.

ACKNOWLEDGMENTS. A typed version of the Thomas Hirst diaries is held at the Royal Institution in London, and quotations from the diaries appear here by courtesy of the Royal Institution. The diaries have been edited by W. H. Brock and R. M. MacLeod, and were published in microfiche by Mansell, London, in 1980.

The Open University
Milton Keynes MK7 6AA
England

Bisectors of Triangles and Tetrahedra

W. A. Beyer and Blair Swartz

1. INTRODUCTION. Our principal goal is to discuss and illustrate (in FIGURES 2, 3 and 4) the envelope of the planes that bisect a tetrahedron. To bisect, here, means to divide into two pieces of equal volume. The envelope of the hyperplanes that bisect a simplex in R^n and the envelope of the lines dividing a triangle into two pieces of fixed relative size are also considered (the last in FIGURE 5). These problems arose in work in numerical hydrodynamics dealing with approximating, within local second-order accuracy, a smooth boundary separating a black and white region in the plane, given discretely located gray values associated with a blurring of that interface (Swartz [17], exemplified at the end of §8 below). But the problems have a much older history in hydrostatics and naval architecture, as they are also connected with the orientation and stability of floating bodies. Favard's book [9] contains a satisfactory discussion of envelopes in R^2 and R^3; there are elementary discussions in Courant [7] or Courant and John [8].

2. A GENERAL DESCRIPTION. The envelope E of the planes that bisect a tetrahedron is homeomorphic to such traditional examples of closed, one-sided surfaces as the "Roman surface" of Steiner (see: Francis [**10**, pp. 83–86], Hilbert and Cohn-Vossen [**12**, pp. 303–4], and Spivak [**15**, pp. 20–1 and p. 34]) and the heptahedron (see Hilbert and Cohn-Vossen [**12**, pp. 302–3] and Jones [**13**]). Indeed, we shall see that the envelope E also consists of seven pieces—it is like a heptahedron whose faces have been pinched to tangency along its edges—but each piece is now part of the zero set of its own polynomial in three variables. In contrast, the Roman surface is the zero set of a single polynomial in three variables that is of total degree four.

3. THE ENVELOPE OF THE BISECTING LINES OF A TRIANGLE. Extending a homework problem in Thomas [**18**, p. 508, #61] or examples in Lamb [**14**, p. 232, Ex. 3], Greenhill [**11**, p. 190], or Bouasse [**6**, §253, p. 382], the following proposition summarizes the information about the envelope of the lines bisecting a triangle.

Proposition. *The envelope E of the set of all lines that bisect a given triangle T is a simple continuous closed curve lying completely inside T. It consists of three parts—the ith part being a segment of a hyperbola whose asymptotes include the two edges containing the ith vertex. Each segment joins continuously with its neighbor to form a cusp where the two are mutually tangent to an intervening median of T—and each of E's three cusps has the same order of sharpness as the graph of $y = |x|^{1/2}$ near $(0,0)$. The expression $b_0V_0 + b_1V_1 + b_2V_2$ for the ith part of the envelope $(i = 0,1,2)$, in terms of barycentric coordinates (b_0, b_1, b_2) relative to the vertices V_0, V_1, V_2 of T, is independent of T and is given by the usual requirement $b_0 + b_1 + b_2 = 1$ together*

with the special requirements

$$8\prod_{\substack{j=0\\ j\neq i}}^{2} b_j = 1 \quad \textit{and} \quad 1/4 \leq b_j \leq 1/2 \quad \textit{for } j \neq i; \tag{3.1}$$

for which $1/4 \leq b_i \leq 1 - 1/\sqrt{2}$. *See* FIGURE 1.

Proof: We first recall an instance of an envelope's hyperbolic segment. The rest then follows using properties of nonsingular affine transformations.

The area of the right triangle $T(x)$, associated with the two coordinate axes and the line tangent to the hyperbola $H := \{(t, 1/t),\ t > 0\}$, is 2, independent of the point $(x, 1/x)$ $(x > 0)$ of tangency. This is a consequence of the following argument. $T(x)$ consists partly of the $x \times 1/x$ rectangle whose diagonal is the radius vector to the point of tangency. And, as the magnitude of the tangent line's slope is $1/x^2$, the interior of $T(x)$ outside this rectangle consists of two $x \times 1/x$ right triangles.

Consider also, now, the isosceles right triangle T_4 of area 4 with vertices $V_0 := (0,0)$, $V_1 := (2\sqrt{2}, 0)$, and $V_2 := (0, 2\sqrt{2})$. The envelope of the hypotenuses of those $T(x)$ that are completely inside T_4 is a portion of the envelope of the bisecting lines for T_4. It is also a segment S of H inside T_4. The right-most point of S is the point $P_r := (\sqrt{2}, 1/\sqrt{2})$ since the tangent line to H here is also the median of T_4 that passes through $(0, \sqrt{2})$ and the vertex V_1. By symmetry, S's left-most point is $P_l := (1/\sqrt{2}, \sqrt{2})$; and the tangent to H there is also the median of T_4 through V_2. Since the curvature of H exists on H but vanishes nowhere, S has the

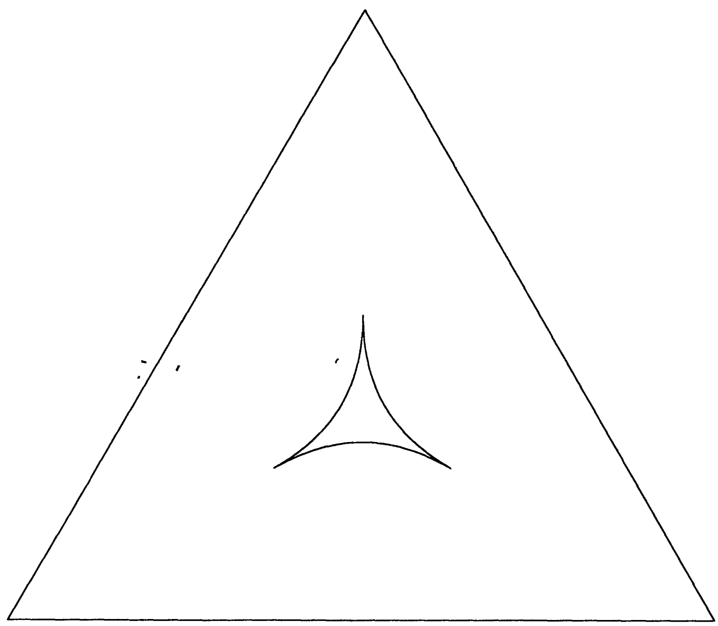


Figure 1. The bisecting envelope of a triangle: a line tangent to the cusped figure separates a corner from its opposite side and divides the triangle into two equal areas. The envelope's vertices are associated with the triangle's. Note that the normal line changes continuously along the whole of the envelope.

type of contact with these two tangent medians that is characteristic of a circle's contact with its tangent—this will be relevant to the cusp's order of sharpness.

Two of the barycentric coordinates of $(x, 1/x)$ with respect to the three vertices V_0, V_1, and V_2 of T_4 are clearly $b_1 = x/(2\sqrt{2})$ and $b_2 = 1/(2x\sqrt{2})$. Consequently, on the segment S, b_1 and b_2 satisfy (3.1) with $i = 0$.

Now: a nonsingular affine map A maps tangent curves onto tangent curves and envelopes of curves onto envelopes of their images. Such a map A also maps lines onto lines, hyperbolas onto hyperbolas, non-degenerate triangles onto non-degenerate triangles and their medians onto medians, and (because A's Jacobian determinant is independent of location) a line that bisects a triangle onto a line that bisects its image. Moreover, since a nonsingular affine map A is the sum of a linear map and a constant vector, the barycentric coordinates of a point V with respect to three points V_0, V_1, and V_2 in general position (non-degenerate convex hull) are also the barycentric coordinates of $A(V)$ with respect to $A(V_0)$, $A(V_1)$, $A(V_2)$ (which are also in general position).

With this, proof of the remainder of the Proposition goes as follows. (a) Use three separate affine maps of T_4 onto an equilateral triangle T_3 (along with the symmetries of T_3) to show that the complete envelope for T_3 satisfies the Proposition (in particular, that neighboring hyperbolic segments are tangent at a common point on a median and so form the cusp as there characterized). (b) Then use a single affine map taking T_3 onto T.

4. PART OF THE ENVELOPE OF THE BISECTING HYPERPLANES OF A SIMPLEX IN *n*-DIMENSIONS.

For $n > 2$ dimensions, consider the surface $H := \{x = (x_1, \dots, x_n) > 0$ such that $f(x) = 0$ with $f(x) := \prod_{j=1}^{n} x_j - 1\}$ (for three dimensions, see, e.g., Appell [**1**, p. 231, problem 11], Greenhill [**11**, p. 202], Struik [**16**, p. 73, problem 6], Courant and John [**8**, problem 8, p. 307]). Note that the jth component of the gradient ∇f of f on H is $(\nabla f)_j = 1/x_j$; hence points X in the hyperplane tangent to H at x satisfy $X \cdot \nabla f = n$. Thus the altitudes of the simplex $S(x)$ bounded by the coordinate hyperplanes and the hyperplane tangent to H at x are $(nx_j)_1^n$; so the volume of $S(x)$ is $n^n/n!$ independent of x. Restricting x so that $S(x) \subseteq S_2 :=$ the simplex of volume $2n^n/n!$ bounded by the coordinate hyperplanes and the hyperplane through and normal to $(1, \dots, 1)$—that is, restricting the vertices of $S(x)$ to lie between those of S_2 and the origin—one can prove (see the Appendix) that an n-dimensional analog of the Proposition in §3 is:

Proposition. *Let $n \geq 2$. The envelope of the hyperplanes bisecting an n-dimensional simplex with vertices $V_0, \dots, V_n$ consists partly of $n + 1$ hypersurfaces, each of degree n. The asymptotic hyperplanes of the ith of these hypersurfaces (some $0 \leq i \leq n$) are the hyperplane extensions of those n faces of the simplex that contain the ith vertex V_i. This ith hypersurface's $n + 1$ barycentric coordinates $b_0, \dots, b_n$ with respect to $V_0, \dots, V_n$ satisfy the usual requirement $\sum_{j=0}^{n} b_j = 1$, together with the relations*

$$2n^n \prod_{\substack{j=0 \\ j \neq i}}^{n} b_j = 1 \quad \text{and} \quad 1/(2n) \leq b_j \leq 1/n \quad \text{for } j \neq i; \tag{4.1}$$

for which $1/(2n) \leq b_i \leq 1 - (2^{-1/n})$. For $n = 3$ dimensions, see FIGURE 2.

The n-dimensional simplex has $n + 1$ vertices. The hyperplanes whose envelope is given by (4.1) separate the ith vertex from the n remaining vertices. Thus there are $n + 1$ such portions of the complete envelope of the simplex's bisecting

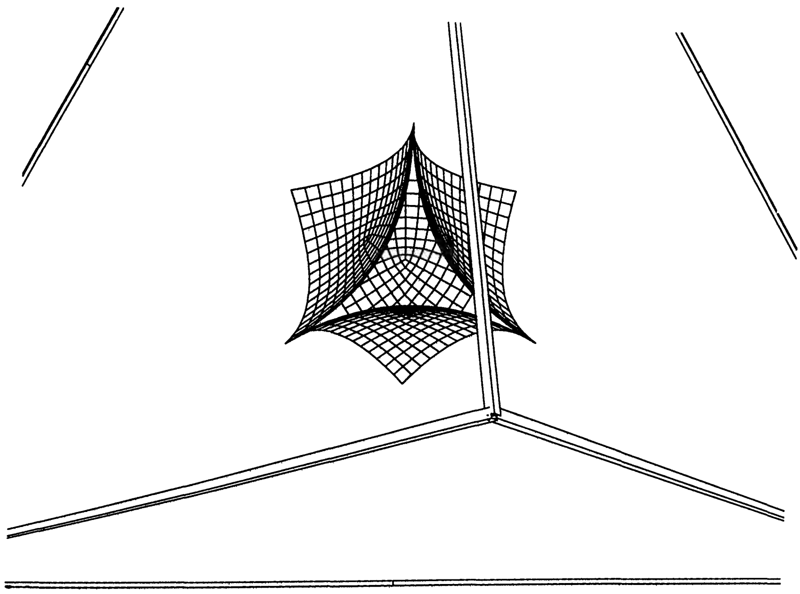


Figure 2. The corresponding bisecting envelope of a tetrahedron: a plane tangent to any of these four cupped, tri-edged surfaces separates a vertex from its opposite face and bisects the tetrahedron. It is now three *edges* of the envelope—the nearest coplanar hyperbolas—that are associated with the tetrahedron's nearest vertex. There must be more bisecting planes.

hyperplanes. But there are other parts of the envelope. To obtain the remaining portions, the following outline of an algorithm can be carried out.

Let the $n + 1$ vertices be divided into two nonempty sets of vertices. Call the total number of such divisions $I(n)$ $(= (2^{n+1} - 2)/2)$. For each such division, it is necessary to find the corresponding portion of the complete envelope. The complete envelope will then consist of $I(n)$ portions. In the next section we discuss the case $n = 3$; it is the only case for which we have a complete discussion.

5. THE ENVELOPE OF THE BISECTING PLANES OF A TETRAHEDRON. A little thought concerning the equilateral tetrahedron ($n = 3$) in this context suggests that, corresponding to each non-intersecting pair of its edges, there should be a saddle-shaped surface bounded by four curves. One of these curves bounding a given saddle coincides with one of the three curves bounding a "cup" of Figure 2—each saddle is thereby connected to each of the four cups. The three saddles intersect (at the center of symmetry, for example) but are not tangent to each other—while they *are* tangent to the cups. Figures 3–4 illustrate these additional steps in the construction of the entire envelope of the bisecting planes of a regular tetrahedron. The captions explain the figures.

Further analysis is required to precisely specify these surfaces. As already noted, the affine invariance of the problem means that it suffices to determine the barycentric coordinates of the complete envelope E of the bisecting planes for any particular tetrahedron, and we shall fix on the tetrahedron U whose vertices are the origin $V_0 := \mathbf{0}$ and the three coordinate unit vectors $V_1 := \mathbf{i}$, $V_2 := \mathbf{j}$, and $V_3 := \mathbf{k}$. In other words, $U = \overline{\mathbf{0ijk}}$, where the overbar means "convex hull of." In this context, if a portion of this envelope is a surface

$$x = x(u,v), \qquad y = y(u,v), \qquad z = z(u,v);$$

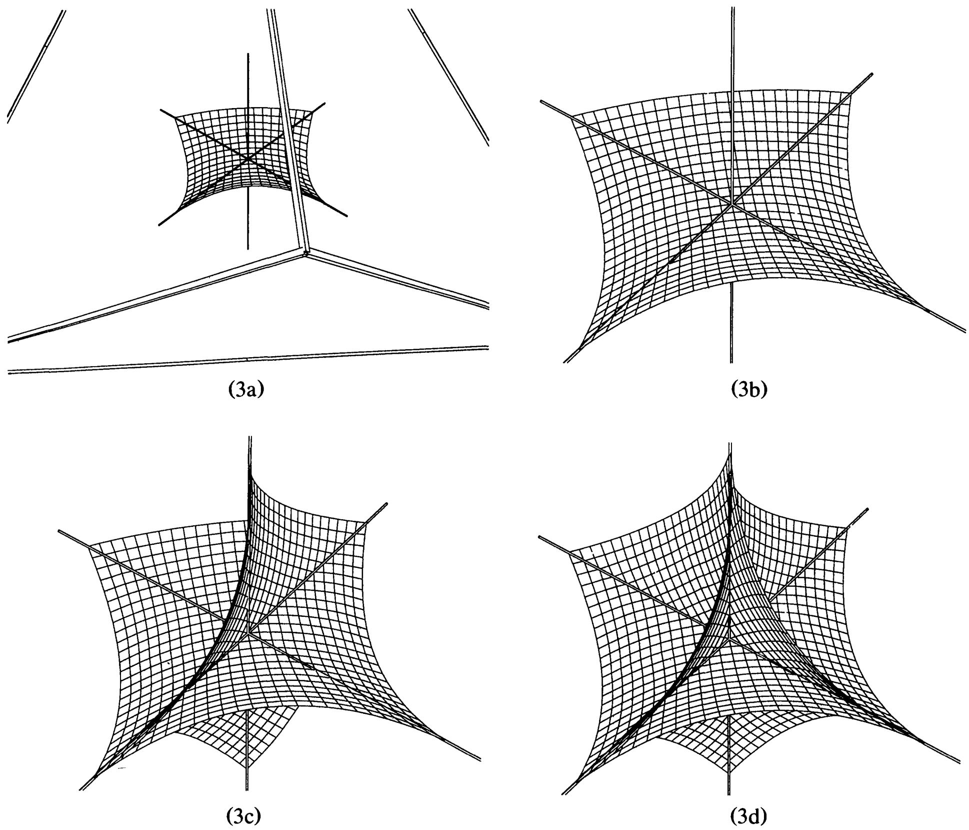


Figure 3. Planes tangent to one of three *saddle*-shaped surfaces bisect the tetrahedron and separate opposing *edges*. The saddles in each pair are tangent at the ends of the line-segment along which they intersect; but at the segment's midpoint (the tetrahedron's centroid) they are orthogonal—this last, for the regular tetrahedron illustrated.

then its associated barycentric coordinates (with respect to $V_0, \ldots, V_3$) will be

$$b_1 = x, \qquad b_2 = y, \qquad b_3 = z, \quad \text{and} \quad b_0 = 1 - (b_1 + b_2 + b_3).$$

For example: according to (4.1), that portion of E consisting of the envelope of the bisecting planes that separate the face $\overline{\mathbf{ijk}}$ from the origin is the surface

$$xyz - 1/54 = 0 \quad \text{with } 1/6 \le x, y, z \le 1/3; \tag{5.1}$$

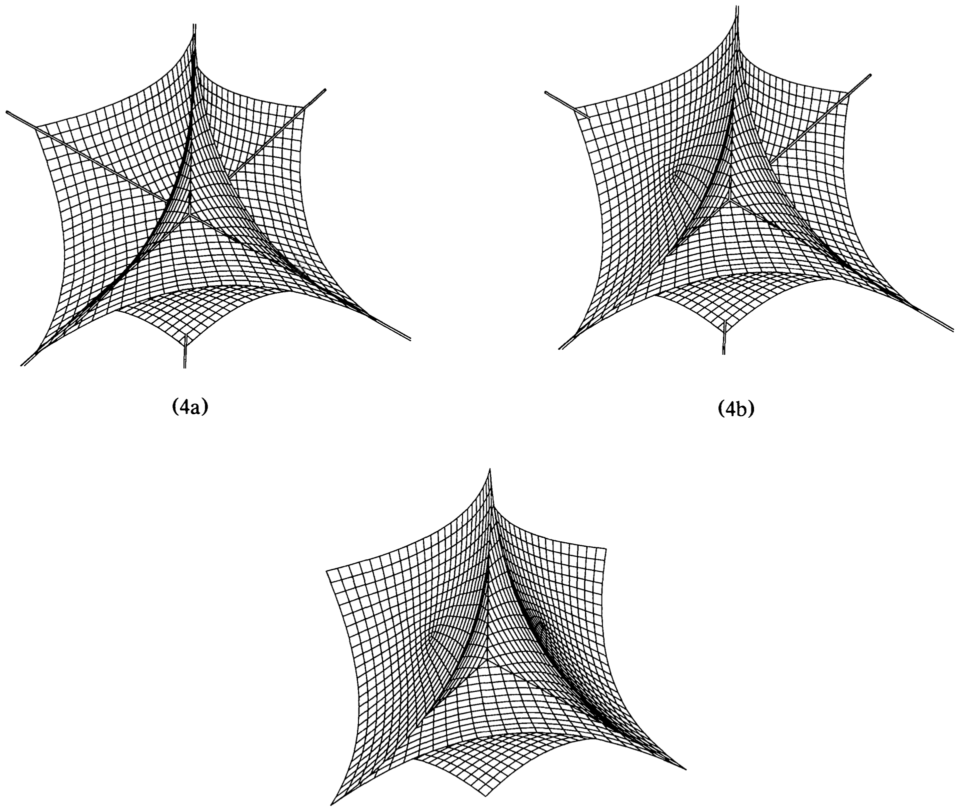
and three other portions of E are found be replacing $x = b_1$, $y = b_2$, and $z = b_3$ here with the three other groups of the four things $\{b_0, \ldots, b_3\}$ taken three at a time.

So it remains to obtain a more analytic description of, say, the envelope of the bisecting planes that separate the edge $\overline{\mathbf{0k}}$ from the edge $\overline{\mathbf{ij}}$; as the remaining two portions of E can then be found by substituting each of the two remaining groups of variables associated with each of the other two pairs of edges.

For this we recall that the envelope of a two-parameter family of surfaces

$$g(x, y, z; p, q) = 0$$

can be constructed by requiring that at the same time g_p $(:= \partial g/\partial p) = 0$ and $g_q = 0$; thereby determining the envelope in the form (say) of $x = x(p, q)$, $y =$



(4a) (4b)

(4c)

Figure 4. The three saddles fit inside the four cups, thus completing the bisecting envelope of a tetrahedron. Each cup is a cubic. Although each saddle is algebraic, its degree is unknown. If the saddles are regarded as *not* intersecting, then the complete envelope (4c) has the topology of Steiner's *Roman surface*—i.e., of Hilbert and Cohn-Vossen's *heptahedron*. And if part of being an envelope is that the normal line change *continuously*, then the saddles *should* be regarded as not intersecting except at their corners.

$y(p,q)$, and $z = z(p,q)$. We shall do this in the slightly different situation of the three-parameter family of surfaces

$$G(x, y, z; p, q, r) := xp + yq + zr - 1 = 0 \tag{5.2}$$

constrained by a known (albeit yet to be described) function

$$F(p,q,r) = 0 \quad \text{determining } r = r(p,q). \tag{5.3}$$

Here one may verify—with a solution of this last in hand—that the functions $x(p,q)$, $y(p,q)$ and $z(p,q)$ given by

$$x = F_p/(pF_p + qF_q + rF_r), \tag{5.4a}$$

$$y = F_q/(pF_p + qF_q + rF_r), \quad \text{and} \tag{5.4b}$$

$$z = F_r/(pF_p + qF_q + rF_r), \tag{5.4c}$$

indeed solve $0 = g = g_p = g_q$ if we define

$$g(x, y, z; p, q) := G(x, y, z; p, q, r(p, q))$$

as specified in (5.2). The relations (5.4) come about as follows: Eliminating r_p between the p-derivative of (5.2) and that of (5.3) yields

$$x = zF_p/F_r; \quad \text{and so, similarly, } y = zF_q/F_r. \tag{5.5}$$

Substituting (5.5) into (5.2) yields the third relation in (5.4); the first two then follow from (5.5). Favard [**9**, p. 186] develops relations equivalent to (5.4) in the context of (5.2)–(5.3), albeit under the assumption that F is homogeneous in variables related to those in (5.2).

It remains to construct a function F so that (5.3) implies that the envelope of (5.2) is the envelope of the bisecting planes separating $\overline{\mathbf{0k}}$ from $\overline{\mathbf{ij}}$. For this it is more convenient to consider the three coordinate-axis intercepts

$$u := 1/p, \qquad v := 1/q, \qquad w =: 1/r \tag{5.6}$$

of the plane (5.2) regarded—for each fixed u, v, and w—as a surface P in xyz-space. This plane P is to separate the edges mentioned, so we take

$$0 < u, v < 1, \quad \text{and} \quad 1 < w < \infty.$$

The volume of the original tetrahedron U is $1/6$, while the volume of the tetrahedron T bounded by P and the three coordinates planes is $uvw/6$. The relationship $F = 0$ (5.3) is to express the bisection requirement that the amount of T inside U be $1/12$. This quantity, $\mathrm{vol}(T \cap U)$, is computed by finding the intersection of P with the edge $\overline{\mathbf{ik}}$ and with the edge $\overline{\mathbf{jk}}$, and subtracting from T's volume the volume of the tetrahedron inside T but outside U using a sixth of the appropriate scalar triple product. Applying (5.6), the associated F we used in (5.3) was

$$F = r^2 + [p + q - 6 + 2/(pq)]r + 6 - pq - 2(p + q)/(pq), \tag{5.7}$$

$$1 < p, q < \infty, \tag{5.8}$$

and such that

$$0 < r < 1. \tag{5.9}$$

That F here, for p and q given, is quadratic in r facilitates the determination of $r(p, q)$ in (5.3) and the associated surface (5.4). Condition (5.9) is actually a condition on p and q. This actually determines only half of the barycentric coordinates of this sheet of the complete envelope E. The remaining half of the sheet is given by interchanging b_3 $(= z)$ and b_0 (this is most easily seen by considering the regular tetrahedron instead of U—a context in which the saddle-shaped character of this sheet is also most apparent). Finally, two other sheets are similarly associated with the other two pairs of edges.

6. THE DEGREES OF THE POLYNOMIALS THAT DESCRIBE THE ENVELOPE. To review: the envelope of the bisecting planes of the tetrahedron has seven parts: three saddle-shaped surfaces and four cup-shaped surfaces. Each of the three saddle-shaped surfaces is associated with separating two edges of the tetrahedron. Each of the four cup-shaped surfaces similarly divides a vertex from a face. We have given the polynomials for the cup-shaped surfaces in (5.1) and its following three lines—they are of total degree three.

We now discuss the polynomials that define the three saddle-shaped surfaces. These polynomials seem to be complicated and we have not been able to complete

this project. The *modus operandi* to find one of these polynomials is to begin with four algebraic equations from §5 in the variables x, y, and z and the parameters p, q, and r. Then one uses resultant theory (see Uspensky [**19**, Chapter XII]) to eliminate the parameters one by one and terminate with one algebraic equation in the variables x, y, and z. This elimination process was attempted on an 8650 VAX computer using the MACSYMA symbolic manipulation system—but it did not complete the final elimination in many days of standby computer time.

More specifically, using (5.3) and (5.4), we obtain:

$$(pF_p + qF_q + rF_r)x - F_p = 0, \tag{6.1a}$$

$$(pF_p + qF_q + rF_r)y - F_q = 0, \tag{6.1b}$$

$$(pF_p + qF_q + rF_r)z - F_r = 0, \tag{6.1c}$$

$$F = 0. \tag{6.1d}$$

We then substitute into the equations (6.1) the expression for F given by (5.7) and clear fractions to obtain a set of four polynomial equations in the variables x, y, and z and parameters p, q, and r. The parameters are subject to the conditions in (5.8) and (5.9). Again, the condition (5.9) is actually a restriction on p and q. The conditions on p and q have no relevance to the resultant algorithm, which treats the parameters to be eliminated as formal symbols. The restrictions (5.8) and (5.9) arise geometrically. However, they are also algebraic restrictions. We know, for example, that if $r = p = q = 1$, then $F = F_p = F_q = F_r = 0$ and the four equations (6.1a–d) are satisfied regardless of the values of x, y, z. Thus all points in R^3 would be on the surface defined by (6.1) for the values $r = p = q = 1$.

To eliminate p, q, and r from (6.1) requires three applications of the resultant calculation. We had enough machine time to do two of the three. We outline these two using the tables below.

The left side of each equation in (6.1) is multiplied by its denominators' least common multiple, yielding polynomials $f^{(1)}(x, p, q, r)$, $f^{(2)}(y, p, q, r)$, $f^{(3)}(z, p, q, r)$, and $f^{(4)}(p, q, r)$. Their degrees and number of terms are displayed in Table 1. This is the first set of equations to which we apply the resultant operation.

TABLE 1

Equation	Degree	# of terms
$f^{(1)}(x, p, q, r) = 0$	6	12
$f^{(2)}(y, p, q, r) = 0$	6	12
$f^{(3)}(z, p, q, r) = 0$	6	13
$f^{(4)}(p, q, r) = 0$	4	9

Eliminating r from the appropriate pairs of equations in Table 1 yielded Table 2.

TABLE 2

Equation	Degree	# of terms
$g^{(1)}(x, p, q) = 0$	9	21
$g^{(2)}(y, p, q) = 0$	9	21
$g^{(3)}(z, p, q) = 0$	10	39

Eliminating q from the appropriate pairs of equations in Table 2 yielded Table 3.

TABLE 3

Equation	Degree	# of terms
$h^{(1)}(x, y, p) = 0$	32	≈ 500
$h^{(2)}(x, z, p) = 0$	27	≈ 300

Assuming little or no cancellation in the elimination of p from the two equations in Table 3 to obtain a single polynomial equation $P(x, y, z) = 0$, we estimate the degree of P to be 150—and if P has no factors, this seems a surprisingly large degree to be associated with such a simple problem. Unfortunately, the MACSYMA computation attempting this elimination was terminated (without output) after many days of calculation.

On the other hand, C. de Boor felt he could demonstrate a lower bound on the saddle's degree [**4**]. For this he took $N \approx 45$ points on the horizontal saddle associated with the tetrahedron having as vertices the points $(\pm(3,3),3)$ and $(\pm(3,-3),-3)$—the resulting saddle has *its* corners at $\pm\mathbf{i}$ and $\pm\mathbf{j}$. He applied a numerical algorithm, based on [**5**], to construct a space $\mathscr{Q}$ of polynomials in three variables of smallest possible degree that allowed unique interpolation to arbitrary values at the N points and at the additional point $(1, -1, 1)$. Although $\mathscr{Q}$ turned out to contain all quartics, he found that nontrivial members of $\mathscr{Q}$ vanishing at the first N points had degree higher than four. This convinced us that the surface defined by (6.1) and (5.7) is of degree higher than four.

7. GRAPHS OF THE ENVELOPE OF THE BISECTING PLANES OF A TETRAHEDRON. For those who care about graphics as well as graphs: The principal software invoked in the computer construction of FIGURES 2–4 was the PLTN2 "super-package," developed by J. M. Hyman and R. Dougherty to ease (interactively) the application of both M. Prueitt's GRAFIC package (used here) and the NCAR (National Center for Atmospheric Research) package. All people mentioned in this connection were at the Los Alamos National Laboratory. GRAFIC plots a sequence of surfaces in three dimensions, each surface being prescribed by a "logically rectangular" set of points $(\mathbf{X}_{ij})_{i=1}^{m}{}_{j=1}^{n}$ lying in the surface. The surface is then approximated as follows. The smallest logical sub-squares are each edged by line segments; and (for the purpose of computing normals) the surface spanning these four segments is considered to be the two-parameter bilinear average interpolating the four vertices (which is one of the doubly ruled surfaces containing these vertices). GRAFIC removes points and line segments that are hidden from the viewer by other surfaces, and both shading and color are options. Indeed, the most illuminating version of these figures includes both.

For the figures, the edges of the tetrahedron and the axes through its centroid are specified to be slender tubes (with polygonal sections), not lines. The requirement of logically rectangular data meant that each cup-shaped segment of the envelope is graphed as the union of three four-edged sections. Along the two (adjoining) outer edges of one of these sections, the mesh is relatively uniform (each such edge is also an edge of one of the saddles). But along the other two edges (where these sections join each other) the mesh diminishes like $r^{4/3}$ towards

the center of the cup-shaped segment. This was done to improve the visual smoothness (associated with the fact that each "cup" is, in fact, analytic), and roughly approximates C. de Boor's suggestion to use a coordinate system associated with a conformal map of a 90° angle onto a 120° angle for this purpose.

8. DIVIDING TRIANGLES INTO REGIONS OF UNEQUAL SIZE. The original problem in computational hydrodynamics requires information about the lines (or planes) that divide a region into two subsets of prescribed (and not necessarily equal) relative size.

Towards this end we consider for given θ, $0 < \theta \leq 1/2$, the envelope E_θ of the lines that separate a triangle T into polygons of relative area θ and $1 - \theta$. As in §3, this problem and its solution are invariant under nonsingular affine maps. So, as in §3, it is relevant that there are two equilateral hyperbolas of the form $xy =$ constant such that some of the tangent lines of each cut the right triangle $\overline{\mathbf{0ij}}$ into two such regions. More specifically, these hyperbolas satisfy

$$\text{either} \quad 4xy = \theta \quad \text{or} \quad 4xy = 1 - \theta,$$

depending on whether the θ-fraction lies on the $\mathbf{0}$-side of the tangent line or on its other side. It follows that: *for given θ, $0 < \theta < 1/2$, the envelope E_θ of the lines that divide a triangle T into portions of relative size θ and $1 - \theta$ consists of three pairs of hyperbolic segments. One pair of the three pairs is associated with each vertex V_i of T by having as asymptotes the two edges of T that contain V_i; and the barycentric coordinates of this pair satisfy (with subscripts taken* mod 3) $b_{i-1} + b_i + b_{i+1} = 1$, together with

$$\text{(a)} \quad 4b_{i-1}b_{i+1} = \theta \quad \text{or} \quad \text{(b)}\ 4b_{i-1}b_{i+1} = 1 - \theta. \tag{8.1a}$$

At the ends of each hyperbolic segment (say of type (a) for some $i = i_1$) one switches to another of the other type (i.e., type (b) for some $i \neq i_1$). Hence, the point (b_{i-1}, b_i, b_{i+1}) at the V_{i+1}-end of the type (a)-segment, being also at the V_{i+1}-end of a type (b)-segment, satisfies

$$4b_{i-1}b_{i+1} = \theta, \qquad 4b_ib_{i+1} = 1 - \theta, \quad \text{and} \quad b_{i-1} + b_i + b_{i+1} = 1. \tag{8.1b}$$

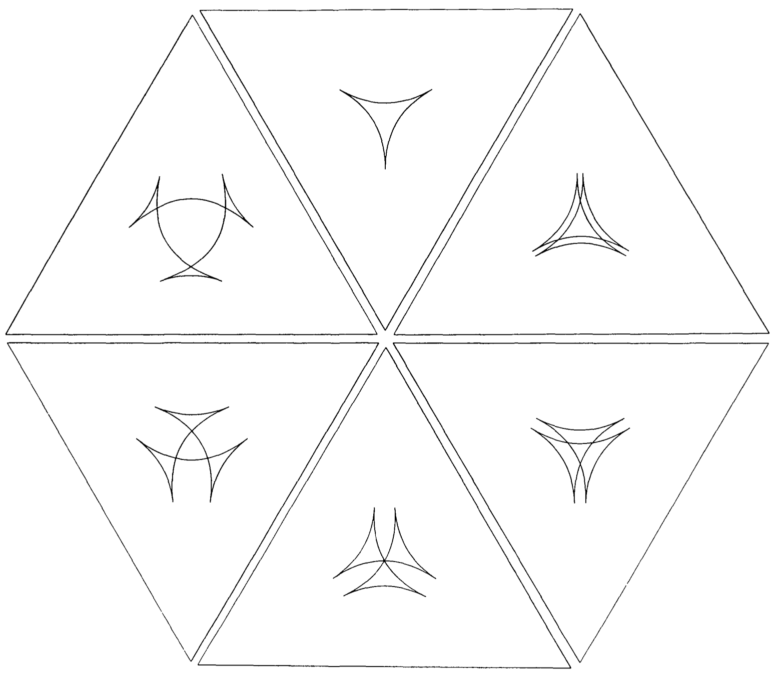
Consequently: *The endpoints of the hyperbolic segments* (8.1a) *or* (8.1b) *also satisfy*

$$b_{i\pm 1} = 1/2 \quad (\text{so that, also, } b_{i\mp 1} + b_i = 1/2 \text{ there}). \tag{8.1c}$$

Checking that, indeed, the two types of hyperbolic segments are tangent at such common points, we see that these cusps (where the interlaced hyperbolic segments now join together with continuously turning tangent line) trace (for $0 < \theta \leq 1/2$) the three open line-segments whose closures connect the three midpoints of the edges of T. And the cusps perform this covering in one-to-one fashion.

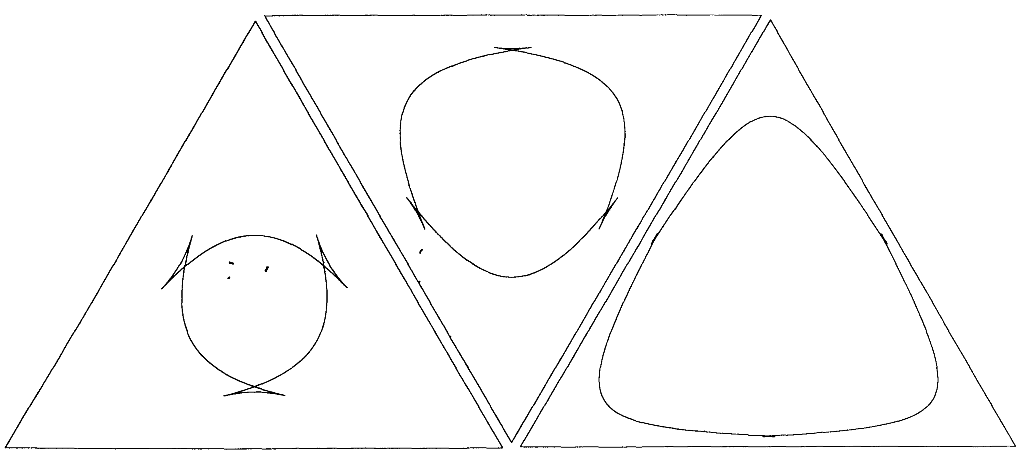
This is all illustrated in FIGURE 5. There it is seen, as θ moves from $1/2$ to 0, that the original three-cusped envelope $E_{1/2}$ (FIGURE 1) doubles its length for θ just below $1/2$, becomes a trefoil containing T's centroid for $\theta = 4/9$; and that E_θ approaches the boundary of the original triangle T as θ approaches zero. Except for $\theta = 1/2$ or $4/9$, the hyperbolas composing E_θ cross (transversely) thrice (each time on one of T's medians), so that it is seen that there is no θ, $0 < \theta \leq 1/2$, such that E_θ bounds only a convex figure.

Let us now illustrate how such envelopes could be used to locally approximate a smooth boundary between a plane region D, colored white, and its black-colored complement, when given as data only the average color $\int_T \chi_D\, dA / \int_T dA$ of each triangle T in a tessellation of the plane into small, equilateral triangles. (χ_D, here,



(5a)

Figure 5. The envelopes of the lines that divide a triangle into two pieces having relative areas θ and $1 - \theta$. Above: clockwise from the top, $\theta = 1/2$, 0.485, 0.47, 4/9, 0.4, and 1/3. Below: from the left, $\theta = 1/4$, 0.15, and 0.05. As the text explains, all curves are segments of hyperbolas whose asymptotes are the sides of the triangle, and all cusps lie on one of the lines joining the midpoints of the original triangle's sides.



(5b)

is the characteristic function of D, and "small" compares the diameter of T to the curvature of the interface). The average color of most triangles will be either black ($= 0$) or white ($= 1$), but those through which the boundary ∂D passes will be colored intermediate values of gray. Since the triangles are small we could hope that a locally liner approximation of ∂D would be second-order accurate (i.e., have an error that goes to zero like the area, not just the diameter, of each triangle). And, indeed, this will be so if (a) the algorithm reproduces an arbitrary linear boundary exactly, and (b) the construction is both local (i.e., determined by nearby data and used only nearby) and stable.

For example: Suppose, in FIGURE 5, that the triangle at 6 o'clock had average color $4/9$ and the triangle at 10 o'clock had average color $2/3$, and that we ignore the remaining triangles. Then there exist only a finite number of lines that divide each triangle into two pieces having areas of appropriate relative size—namely, the four common tangents to the indicated envelopes. But, only two of these four lines will do as borders of a half-space to approximate ∂D; since either of the other two would have to be black on one side in order to color one triangle appropriately, but be white instead on that same side to simultaneously color the other triangle appropriately. Like the sign of a square root, the selection between the two remaining candidates for a linear boundary must be made using an additional criterion—for example, the location of some completely white triangle would usually suffice.

Further details will be found in [**17**], including discussion of geometric circumstances leading to second-order accuracy (and others, to lower-order accuracy in spite of reproducing linear boundaries). That three gray average colors can determine approximating planes in three dimensions is also noted there, along with connections of these problems with polynomial spline functions and with apparently nontrivial generalizations of the "ham-sandwich" problem of Steinhaus.

9. REMARKS. It is worth noting the connection of our envelopes with "surfaces of flotation" (using the terminology of hydrostatics and of naval architecture). Thus, suppose one is given a body K in Euclidean n-space along with a prescribed θ in $(0, 1)$. Let E_θ be the envelope of those (hyper)planes dividing K in two parts having relative volume θ and $1 - \theta$. (If the body K had specific gravity θ (or $1 - \theta$) and were floating in some orientation, then its sea-level (hyper)plane section would be tangent to E_θ independent of that orientation.) In this regard, then, White and John [**20**] claim to be the first to recognize (1871) that for two dimensions the complete curve of flotation of an object can contain cusps—indeed, our FIGURE 5 for $\theta = 1/4$ is qualitatively described there quite accurately [**20**, p. 93]. In fact, the curves of flotation (for triangles of unspecified specific gravity) in FIGURES 3, 4 and 5 of their Plate V (kindly sent us by the Secretary of the Royal Institution of Naval Architects) are in harmony with the envelopes E_θ in our FIGURE 5 for $\theta = 4/9$, $1/4$, and $1/3$, respectively. Moreover, the curve of flotation for actual vessels—see, e.g., [**20**, FIGURE 1 of Plave IV] or the reproduction (from another paper by White) in Greenhill [**11**, p. 160]—have many characteristics in common with the curves in our FIGURE 5.

In the expanded version of this paper (the report [**2**]) we included an attempt to use a classic result concerning surfaces of flotation to help demonstrate that the topology of bisecting hypersurfaces $E_{1/2}$ in n-space is that of the projective hyperplane P^{n-1}, but that the topology E_θ for $\theta \neq 1/2$ is, instead, that of the surface S^{n-1} of the unit ball. The attempt fails—but it is both amusing and instructive.

It is possible for the envelope of the bisecting hyperplanes of a region to be a single point—consider a rectangle or a circular disc. When it exists we have called such a point a halfway point (all this in another report [**3**]). There we extend the concept—i.e., of the notion of the median of a distribution—as follows. Let ρ be a nonnegative function on R^n whose integral R^n is finite. Then a point h in R^n is called the *halfway point* for ρ if any $(n-1)$-dimensional hyperplane H containing h has half the mass of ρ on each side: i.e.

$$\int_{H^+} \rho(x)\,dx = \int_{H^-} \rho(x)\,dx,$$

where H^+ and H^- denote the two half spaces on either side of H. In [**3**] we consider some characteristics of functions ρ that have halfway points.

ACKNOWLEDGMENTS. The authors wish to thank the following people for fruitful discussions and help: C. de Boor, E. Calabi, G. D. Chakerian, R. Dougherty, R. Hersh, H. B. Lawson, R. D. Mauldin, and J. Mycielski. The U.S. Department of Energy supported our work.

APPENDIX. FINISHING THE PROOF OF THE PROPOSITION IN §4. Let e_j be the jth coordinate unit vector in the canonical basis for R^n. Note that a point $\xi = \Sigma_{j=1}^n \xi_j e_j$ in R^n then has *barycentric* coordinates $(b_0, b_1, \dots, b_n)$ relative to the $n+1$ vectors $e_1, \dots, e_n$, and the origin $0 =: e_0$ that are given by $b_1 = \xi_1, \dots, b_n = \xi_n$, and $b_0 := 1 - \Sigma_{j=1}^n b_j$; for then $\xi = \Sigma_{j=0}^n b_j e_j$ with $\Sigma_{j=0}^n b_j = 1$. With this the tangent hyperplane at a point $b = \Sigma_{j=1}^n b_j e_j$ in the hypersurface G of points $b > 0$ satisfying $g(b) := \Pi_{j=1}^n b_j - 1/(2n^n) = 0$ (see (4.1) with $i = 0$), namely the hyperplane H_b of points $B = \Sigma_{j=1}^n B_j e_j$ satisfying $\Sigma_{j=1}^n (B_j/b_j) = n$, defines (with the n coordinate hyperplanes) a simplex Σ_b whose volume is half that of the standard simplex $\Sigma := \overline{e_0 e_1 \dots e_n}$ (the overbar here means "convex hull of"). (To see that g is indeed an appropriately scaled version of the function f in the discussion above the Proposition in §4—and thus that the equation in (4.1) is correct—note that the simplex S_2 being bisected there is the convex hull of the origin $0 =: w_0$ and the n vectors $w_j := n2^{1/n} e_j$, $1 \le j \le n$; so that for x there to satisfy both $x = \Sigma_{j=1}^n x_j e_j$ and its barycentric expression $x = \Sigma_{j=0}^n b_j w_j$ relative to $w_0, \dots, w_n$ it suffices that $g(b) = 0$ and $\Sigma_{j=0}^n b_j = 1$.)

The upper bounds $1/n$ in the inequalities $1/(2n) \le b_j \le 1/n$ in (4.1) are simply the additional constraints on b in G appropriate for H_b to bisect Σ; i.e., for Σ_b to be completely contained in Σ; i.e., for each of H_b's n coordinate-axis intercepts nb_j to lie between 0 and 1. The lower bounds $1/(2n)$ on all but b_0 come about as follows: Fix k, $1 \le k \le n$. Then b_k satisfying $g(b) = 0$ attains its minimum relevant value $b_k = 1/(2n)$ when the b_j, $1 \le j \le n$ but $j \ne k$, all take on their maximum relevant values $1/n$—and note, for this b in G, that b_0 is also $1/(2n)$.

Finally, we now shall see that b_0 can be no smaller than $1/(2n)$ for all b in the "bisecting subset" $G_{1/2} \subset G$ (i.e., when $\Sigma_b \subset \Sigma$). Equivalently, we shall show that $L(b) := \Sigma_{j=1}^n b_j$ is maximized on $G_{1/2}$ when $g(b) = 0$ (of course) and all but one of $b_1, \dots, b_n$ are $1/n$. First: as $\nabla L = \Sigma_{j=1}^n e_j$, L has only one extreme value on the hypersurface G—namely, when all nb_j are $1/(n2^{1/n})$—and it is a minimum (namely, $2^{-1/n}$). Consequently, maxima for L over $G_{1/2}$ occur on its boundary. But b lies in the boundary of $G_{1/2}$ if and only if at least one b_j is $1/n$, i.e., at least one of the intercepts nb_j of the corresponding bisecting hyperplane H_b is 1. (For if all nb_j are strictly between 0 and 1—and also restricted by $g(b) = 0$ of course—then b is in the interior of $G_{1/2}$ in that the intercepts of H_b then have $n-1$ independent degrees of freedom locally.) So, suppose $b_n = 1/n$. Then we

wish to maximize $L_{n-1}(b_1, \ldots, b_{n-1}) := \Sigma_{j=1}^{n-1} b_j$ subject to $g_{n-1}(b_1, \ldots, b_{n-1}) := \Pi_{j=1}^{n-1} b_j - 1/(2n^{n-1}) = 0$. The one interior extremum is again a minimum (with all $n-1$ variables now $1/(n2^{1/(n-1)})$); the boundary containing the maxima again consists of vectors with at least one more intercept of H_b being 1, i.e., with one more coordinate, say b_{n-1}, being fixed at $1/n$. And so forth, down to the point when $L_2(b_1, b_2) := b_1 + b_2$ is to be maximized subject to $g_2(b_1, b_2) := b_1 b_2 - 1/(2n^2) = 0$. Hence (say) $b_2 = 1/n$ and $b_1 = 1/(2n)$. And we have shown what we desired—namely, that the maxima of L over $G_{1/2}$ (and hence the minima $1/(2n)$ of b_0) occur with $b_j = 1/(2n)$ for some $1 \le j \le n$, and all the rest at $1/n$.

Geometrically, these extrema occur when the hyperplane H_b that bisects Σ also contains one of the $(n-2)$-dimensional "edges" of the "face" $\overline{e_1 e_2 \ldots e_n}$ of Σ that H_b is separating from the vertex e_0—each of these n "edges" consists of the convex hull of all but one of the basis vectors $e_1, \ldots, e_n$.

The minimization of b_0 above is a simple example of solving a problem in *geometric programming*, that is, finding the extreme values of a generalized polynomial in n variables subject to generalized polynomial constraints. A generalized polynomial, here, is a linear combination of products of (not necessarily integral) powers of the variables.

Added in Proof. Our text associates the idea of the heptahedron with the names of Hilbert and Cohn-Vossen. However, François Aprèy's recent and handsome book, *Models of the Real Projective Plane* (Friedr. Vielag & Sohn, Braunschweig, 1987), calls it (p. 17) the *Reinhardt heptahedron*. An appropriate reference is: Curt Reinhardt, Zu Möbius' Polyedertheorie, Berichte über die Verhandlungen der Königlichen Sächsischen Gesellschaft der Wissenschaften zu Leipzig, Mathematisch-physikalische Classe, vol. 37, 1885, pp. 106–125. Reinhardt also deposited a cardboard model in the Mathematical Institute of the University at Leipzig. We do not know if it survived.

REFERENCES

1. P. Appell, *Équilibre et mouvement des milieux continus*, Traité de mécanique rationnelle, vol. 3, 3rd edition, Gauthier-Villars, Paris, 1921.
2. W. A. Beyer and B. Swartz, *The envelope of the planes that bisect a tetrahedron*, Los Alamos report LA-UR-90-2491, (July, 1990).
3. W. A. Beyer and B. Swartz, *Halfway points*, SIAM J. Math. Anal., 23 (1992), 1332–1341.
4. C. de Boor, private communication, 1990.
5. C. de Boor and A. Ron, *On multivariate polynomial interpolation*, Constr. Approx. 6 (1990), 287–302.
6. H. Bouasse, *Hydrostatique: Manomètres, baromètres, pompes*; *Équilibre des corps flottants*, Libraire Delagrave, Paris, 1923.
7. R. Courant, *Differential ahd Integral Calculus*, vol. 2, Interscience, New York, 1961.
8. R. Courant and F. John, *Introduction to Calculus and Analysis*, vol. 2, Wiley-Interscience, New York, 1974.
9. J. Favard, *Cours de géométrie différentielle locale*, Gauthier-Villars, Paris, 1957.
10. G. K. Francis, *A Topological Picturebook*, Springer-Verlag, New York, 1987.
11. A. G. Greenhill, *A Treatise on Hydrostatics*, Macmillan, London, 1894.
12. D. Hilbert and S. Cohn-Vossen, *Geometry and the Imagination*, Chelsea, New York, 1952, (Translation of "Anschauliche Geometrie," J. Springer, Berlin, 1932, which was reprinted by Dover in 1944).
13. R. H. Jones, Folding polyhedra, *Structural Topology* 7 (1982), 45–50.
14. H. Lamb, *Statics: Including Hydrostatics and the Elements of the Theory of Elasticity*, 3rd edition, Cambridge Univ. Press, Cambridge, 1928.
15. M. Spivak, *A Comprehensive Introduction to Differential Geometry*, vol. 1, 2nd edition, Publish or Perish, Berkeley, CA, 1979.

16. D. J. Struik, *Differential Geometry*, Addison-Wesley, Cambridge, MA, 1950.
17. B. Swartz, *The second-order sharpening of blurred smooth borders*, Mathematics of Computation 52 (1989), 675–714.
18. G. B. Thomas, *Calculus and Analytic Geometry*, 3rd edition, Addison-Wesley Co., Reading, MA, 1960.
19. J. V. Uspensky, *Theory of Equations*, McGraw-Hill, New York, 1948.
20. W. H. White and W. John, *On the calculation of the stability of ships, and some matters of interest connected therewith*, Trans. Royal Institution of Naval Architects (1871), 77–127, (esp. Plates IV, V, and VI—but, "The drawings, not published with the paper, are in the possession of the Institution, and can at any time be seen by members in the Library.—ED.", according to Trans. I. N. A., 1884, p. 74).

Los Alamos National Laboratory
T Division, MS-B284
Los Alamos, NM 87545
beyer@lanl.gov; bks@lanl.gov

Postscript. We've just been pointed (by L. M. Kelly) to G. Gunther and J. B. Wilker's paper *The bisectrix of a tetrahedron*, Mathematika 39 (1992), 93–103. Although figures and any historical perspective are lacking there, we do want to otherwise note a number of similar ideas.

The name of Professor FELIX KLEIN, of the University of Göttingen, together with those of six other German educators, has been cancelled from the roll of honorary members of the National Education Association in response to a persistent demand from active members of the association, from members of the Council of National Defense, and from others.

—*American Mathematical Monthly* 25, (1918) p. 331

More on Rectangles Tiled by Rectangles

D. G. Mead and S. K. Stein

The first theorem on a rectangle tiled by rectangles was proved by Dehn in 1903 [3]:

Theorem 1. *Let R be a rectangle that has at least one edge of rational length. Let R be tiled by smaller rectangles each of which has the property that the ratio of its length to its width is rational. Then all the edges of R and of the tiling rectangles have rational lengths.*

In 1940 Brooks, et al. [2] obtained this result by associating an electrical network consisting of currents, voltages, and resistances with the tiling and using well known properties of such networks. We will modify their approach slightly by adding a battery to each edge to obtain the following theorems.

Theorem 2. *Let R be a rectangle that has at least one edge of rational length. Let R be tiled by smaller rectangles each of which has a rational perimeter. Then all the edges of R and of the tiling rectangles have rational lengths.*

If the assumption on R in Theorem 2 is replaced by "R has a rational perimeter," the result is false, as is shown by tiling the $2\sqrt{2}$ by $4 - 2\sqrt{2}$ rectangle by four $\sqrt{2}$ by $2 - \sqrt{2}$ rectangles.

Theorem 3. *Let R be a rectangle that has at least one edge of rational length. Let R be tiled by smaller rectangles whose length and width differ by a rational number. Then all the edges of R and of the tiling rectangles have rational lengths.*

Note that either Theorem 1 or Theorem 3 implies that in a tiling of a rectangle with a rational edge by squares, all the dimensions of the rectangles are rational.

Theorem 4. *Let R be a rectangle whose width and length differ by a rational number. Let R be tiled by smaller rectangles each of which has a rational perimeter. Then all the edges of R and of the tiling rectangles have rational lengths.*

1. THE METHOD. Let G be a connected linear graph with m vertices and n edges, $e_1, e_2, \dots, e_n$, such that each edge is incident to two distinct vertices. There may be more than one edge incident to the same vertices. If edge e_i is incident to the vertices A and B we orient e_i by selecting one of the orientations AB or BA. (We may think of the orientation AB as an arrow from A to B and the algebraic boundary of e_i as $B - A$.).

Let C_1 consist of the formal sums $\Sigma_{i=1}^{n} x_i e_i$, where x_i is real. Such a sum is shorthand for a function h from the set of edges to the real numbers, where

$h(e_i) = x_i$. C_1 is a vector space of dimension n with real coefficients. If the vertices are $V_1, V_2, \ldots, V_m$ let C_0 consist of the formal sums $\Sigma_{i=1}^{m} y_i V_i$ where the y_i are real. This sum stands for a function p from the set of vertices to the real numbers, where $p(V_i) = y_i$. Define ∂: $C_1 \to C_0$ by setting $\partial(e_i) = B_i - A_i$ if e_i is oriented from A_i to B_{ig} and extending by linearity. Note that $p(\partial e_i) = p(B_i - A_i) = p(B_i) - p(A_i)$.

Let $r_1, r_2, \ldots, r_n$ be nonnegative real numbers associated with the edges $e_1, e_2, \ldots, e_n$ respectively such that the set of edges associated with the r_i's that are 0 contains no closed circuit. Let $w_1, w_2, \ldots, w_n$ be n real numbers.

Consider the following two equations for the unknown functions $h \in C_1$ and $p \in C_0$:

$$\text{I.} \qquad \partial\left(\sum_{i=1}^{n} h(e_i) e_i\right) = 0$$

$$\text{II.} \qquad p(\partial e_i) = w_i - r_i h(e_i).$$

(In terms of electrical networks, $h(e_i)$ is the current in e_i, r_i is the resistance in e_i, w_i is the electromagnetic force of a battery attached to e_i and $p(V)$ is the potential at V. Equation I asserts that the total current entering a vertex is 0. Equation II relates the voltage drop over an edge to the current, resistance and the strength of the battery at that edge.)

In ([**1**], 162–171) it is shown that these simultaneous equations have a unique solution for h and a unique, up to an additive constant, solution for p. Actually, in [**1**] it is assumed that all r_i are positive. However, the key argument, which appears in the footnote on p. 171, goes through with our weaker assumptions, as long as the spanning tree used in the proof is chosen to contain the edges for which $r_i = 0$. (There is a misprint in the footnote: the final $\geq$ should be replaced by $>$.) Moreover, the formulas for the values of h and p obtained there show that if r_i and w_i, $1 \leq i \leq n$, are all rational, then so are the values of h and therefore of $p(\partial e_i)$. The same conclusion holds if "nonnegative" is replaced by "nonpositive" in [**1**].

As in [**2**] associate a linear graph with a tiling of a rectangle R by rectangles $R_1, R_2, \ldots, R_{n-1}$. (For convenience, denote R also by R_n.) To do this, introduce an xy coordinate system such that R_n is in the first quadrant, its edges are parallel to the axes, and the origin is at a corner of R. Each rectangle R_i, $1 \leq i \leq n$, has edges parallel to the x-axis (the "horizontal edges") of length h_i and edges parallel to the y-axis (the "vertical edges") of length v_i.

Let S be the union of all the horizontal edges of the n rectangles. The midpoints of the connected components of S will be the vertices of a linear graph G. For each rectangle R_i, $1 \leq i \leq n-1$ introduce an edge oriented from the component containing its lower edge to the component containing its upper edge. For $R_n = R$, introduce an edge oriented from its upper edge down to its lower edge. At a vertex V define $p(V)$ to be the y-coordinate of V. Thus for $1 \leq i \leq n-1$, $p(\partial e_i) = v_i$ and $p(\partial e_n) = -v_n$. Also define $h(e_i)$ to be h_i, $1 \leq i \leq n$.

The definitions of r_i and w_i will depend on the particular theorem to be proved.

2. PROOFS OF THE THEOREMS. The proof of Theorem 1, as given in [**2**], goes as follows. First place R in such a way that its vertical length v_n is rational. Define r_i to be $-v_i/h_i$, $1 \leq i \leq n-1$. Define r_n to be 0. Define w_i to be 0, $1 \leq i \leq n-1$ and w_n to be $-v_n$. Checking that I and II are satisfied is straightforward. Thus, all h_i and v_i, $1 \leq i \leq n$, are rational.

To prove Theorem 2 let $w_i = h_i + v_i$, $1 \leq i \leq n - 1$, and $w_n = -v_n$. Let $r_i = 1$, $1 \leq i \leq n - 1$, and $r_n = 0$.

To prove Theorem 3 first place the rational edge of R along the y-axis. For $1 \leq i \leq n - 1$ let $r_i = -1$ and $w_i = v_i - h_i$. Let $r_n = 0$ and $w_n = -v_n$.

To prove Theorem 4 let $r_i = 1$ and $w_i = h_i + v_i$ for $1 \leq i \leq n - 1$. Let $r_n = 1$ and $w_n = h_n - v_n$.

These theorems could be generalized by assuming, that for each R_i, $1 \leq i \leq n - 1$, there is a positive (negative) rational number r_i such that $v_i + r_i h_i$ is rational and that v_n is rational. The proof is similar.

3. ANOTHER APPROACH. In the proof in [**1**] the values of p, h, and w are never multiplied by each other. Thus we may take their values in a vector space over the field generated by $r_1, \dots, r_n$, in particular in the abelian group $\mathbb{R}/\mathbb{Q}$, under addition. In the proofs w_i is now an element of $\mathbb{R}/\mathbb{Q}$, the zero element. Equations I and II, which refer to elements in $\mathbb{R}/\mathbb{Q}$, hold and again the solution is unique, namely p and h must both be the constant function with value $0 \in \mathbb{R}/\mathbb{Q}$.

For a different type of problem concerning tiling a rectangle by rectangles see [**4**].

REFERENCES

1. D. W. Blackett, *Elementary Topology*, Academic Press, New York, 1967.
2. R. L. Brooks, C. A. B. Smith, A. H. Stone, and W. T. Tutte, The dissection of rectangles into squares, *Duke Math. J.* 7 (1940), 312–340.
3. M. Dehn, Zerlegung von Rechtecke in Rechtecken, *Math. Ann.* 57 (1903), 314–332.
4. S. Wagon, Fourteen proofs of a result about tiling rectangles, *Amer. Math. Monthly* 94 (1987), 601–617.

Mathematics Department
University of California at Davis
Davis, CA 95616-8633

The Birthday Problem

In an article in the January, 1992, issue of the MONTHLY, Joag-Dev and Proschan present an elementary example of the use of majorization in probability. This example considers the Birthday Problem where different dates have different probabilities.

Another frequently taught problem in probability is the Coupon Collector's Problem, and this problem provides a similar elementary example of the use of majorization. Suppose that n objects are picked repeatedly and independently with the probability that object i is picked at on a given try is p_i (where $p_1 + \dots + p_n = 1$). Let $\mathbf{p} = (p_i, \dots, p_n)$ and let $T_{\mathbf{p}}$ be the Coupon Collector's Time, i.e. the earliest time where all n objects have been picked at least once. A reasonable exercise for someone who has read the article of Joag-Dev and Proschan is to show that

$$P(T_{(1/n, \dots, 1/n)} \leq t) \geq P(T_{\mathbf{p}} \leq t)$$

for any $\mathbf{p}$ and to show that $P(T_{\mathbf{p}} \leq t)$ is a Schur-concave function of $\mathbf{p}$.

—*Martin V. Hildebrand*
Department of Mathematics
The University of Michigan
Ann Arbor, MI 48109-1003

Ramanujan—For Lowbrows

Bruce C. Berndt and S. Bhargava

"No, Inspector," he said. "It is not at all like that, I am assuring you. You see, for a person of my sort—and I admit that we are a rare breed—numbers are so much in our minds there is hardly any question of writing them down, let alone adding one to another."...

"Let me give you one instance," he said. "Before I was beginning work just now, I was taking a short stroll, and I happened to see a handcartwalla. Now, being the sort of chap I am, I of course notice the number burned on the side of the cart: seventeen-twenty-nine. Now, does that mean anything to you yourself?"

"It is the number on the cart," Ghote answered guardedly. "By law it must be there."

Raghu Barde smiled his warm smile again.

"Ah, yes, the police view. But what do you think those figures meant to me? You would never guess. But the moment I was seeing them I said: Aha, the smallest number expressible as a sum of two cubes in two different ways. And, you know, if ever I am getting to marry, I suppose I will want a wife whose birth date comes to some number pleasing to me like that."

"I see," Ghote said.

And, although the mumbo jumbo about cubes and expressible meant nothing to him, and he could not help thinking that to choose a wife by number would be a much riskier proceeding than to let the astrologers choose one for you, he did dimly see what a different sort of life Raghu Barde lived from that of the common number-unencumbered man.

H. R. F. Keating
Dead on Time

1. INTRODUCTION. To celebrate the centenary of Ramanujan's birth, in June, 1987, an international conference was held at The University of Illinois at Urbana-Champaign [1]. Numerous roads through varied scenery brought researchers from Ramanujan's papers, problems, letters, notebooks, and unpublished manuscripts to a panoply of areas of contemporary research, including partitions, mock theta-functions, statistical mechanics, Lie algebras, probabilistic number theory, modular forms, elliptic functions, complex multiplication, hypergeometric series, q-series, asymptotic expansions, and beta integrals. Very few mathematicians have ever had such a broad impact on mathematical research. Although many results presented at the conference could be understood and appreciated by mathematicians outside these areas of research, this was a conference for *highbrows*.

Many of Ramanujan's beautiful discoveries, however, are easily understood, are elementary, and appeal to a wide variety of tastes. Thus, this paper is written for *lowbrows*. Only elementary algebra is needed to prove the lion's share of theorems reported here. Most are found in the unorganized portion of Ramanujan's second notebook, his third notebook, and problems that he posed for readers of the *Journal of the Indian Mathematical Society*. The results we describe fall under the headings of elementary algebra, equal sums of powers, and elementary number theory.

We begin our expedition in a taxi-cab as we recount G. H. Hardy's riding in taxi-cab no. 1729 to visit Ramanujan while lying ill in Putney. Some historical remarks are offered on the two representations $1^3 + 12^3 = 9^3 + 10^3$ of 1729. This leads us to Euler's solution, rediscovered by Ramanujan in a simpler form, of the diophantine equation $A^3 + B^3 = C^3 + D^3$.

We turn from equal sums of third powers to equal sums of fourth powers and ask "Did Ramanujan ever read Mathematical Magazine?" No, we are not speaking of the journal, Mathematics Magazine, published by the MAA, with the first issue appearing under a slightly different title in 1926, six years after Ramanujan's death. Some historical remarks will be made about Mathemati*cal* Magazine.

We next temporarily stop our journey to view what the authors consider to be one of the most captivating, enthralling finite identities in all of mathematics. Is this marvelous identity simply an accident on the road to sums of powers? Or are we at the base of the Himalayas—facing away from the mountains?

We next encounter three types of systems of equations. The first system leads us to sequences that decrease for a while, then increase for a while, etc. We must have roamed to a college campus, for these sequences involve radicals, infinitely many of them. Like most radicals, these have interesting properties. The second system leads us to a visit with S. Ramanujam. No, that is not a misprint! Is he really Ramanujan, or is he someone else? Our third system was solved beautifully by Ramanujan in his third published paper, but he did not realize that J. J. Sylvester had solved this system in 1851, nor was Ramanujan aware of the implications of his work. We provide a sketch of Ramanujan's clever proof.

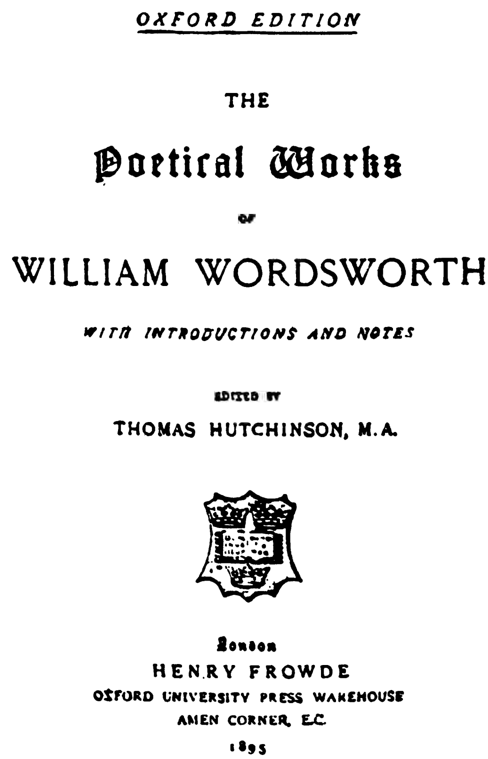
Proceeding from a sketch to a complete landscape, we provide proofs of some interesting properties of roots of cubic polynomials that Ramanujan discovered. As applications, we offer two curious trigonometric identities.

For our last proof, we establish sharp bounds for a sum giving the largest power of a prime dividing $n!$.

We conclude our paper with some approximations to π.

Several references will be made to Ramanujan's notebooks [**26**], published in two volumes. The second volume contains the second and third notebooks, and all page numbers in this paper refer to the pagination in this volume.

2. SUMS OF POWERS. Many readers are familiar with the famous taxi-cab story immortalized by Hardy [**27**, p. xxxv]. "I remember once going to see him when he was lying ill at Putney. I had ridden in taxi-cab no. 1729, and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavourable omen. 'No,' he replied, 'it is a very interesting number; it is the smallest number expressible as a sum of two cubes in two different ways.'" (It is clear that the author of the opening passage about a handcart with 1729 imprinted on its side was acquainted with this delightful incident in the life of Ramanujan and Hardy. A handcartwalla is a person who pulls a two-wheeled handcart, normally carrying one or two people, and is no longer a common sight in present day India. The suffix "walla" comes from Hindi.) In fact, Ramanujan had previously recorded these two representations for 1729, $1^3 + 12^3$ and $9^3 + 10^3$, on page 225 of his second notebook [**26**]. However, this example appears to have been first noticed by B. Frénicle de Bessy in 1657. Frénicle and J. Wallis each found additional examples for two equal sums of two cubes. A bitter argument ensued with each accusing the other of using trivial methods. Since P. Fermat also frequently was feuding with these two men, letters detailing their acrimony can be


OXFORD EDITION

THE

Poetical Works

OF

WILLIAM WORDSWORTH

WITH INTRODUCTIONS AND NOTES

EDITED BY

THOMAS HUTCHINSON, M.A.

London

HENRY FROWDE

OXFORD UNIVERSITY PRESS WAREHOUSE

AMEN CORNER, E.C.

1895

The frontispiece of a volume of Wordsworth's poetry. The volume was awarded to the young Ramanujan for his "outstanding work in Maths." Such prizes for mathematical contests were common in Ramanujan's hometown, Kumbakonan, and throughout India of the period.

found in Fermat's *Oeuvres* [**11**, pp. 419–420; 427–457] and E. T. Bell's book [**2**, Chapter 12], as well as in L. E. Dickson's *History* [**8**, p. 552]. In 1898, C. Moreau [**18**] found the ten solutions of $A^3 + B^3 = C^3 + D^3$ with the sums less than 100,000. After 1729, the next largest sum is $4104 = 2^3 + 16^3 = 9^3 + 15^3$.

From another viewpoint, Ramanujan provided Hardy with solutions to the classical diophantine equation

$$A^3 + B^3 + C^3 = D^3. \tag{2.1}$$

L. Euler [**10**] completely solved (2.1) for positive or negative rational solutions. At three places in his notebooks, Ramanujan addresses the problem of finding solutions of (2.1). In Entry 20(iii) of Chapter 18 and on page 266 in the unorganized portion of his second notebook, Ramanujan provides parametric solutions to (2.1), but they are not as general as Euler's. But near the end of his third notebook [**26**, p. 387], Ramanujan offers a family of solutions equivalent to Euler's general solution. Both Hardy [**13**, p. 11] and G. N. Watson [**30**] discussed one of Ramanujan's less general solutions to (2.1). They had no knowledge of Ramanujan's general solution, because they did not have access to the third notebook. We quote Ramanujan's theorem.

Theorem. *If*

$$\alpha^2 + \alpha\beta + \beta^2 = 3\lambda\gamma^2,$$

then

$$(\alpha + \lambda^2\gamma)^3 + (\lambda\beta + \gamma)^3 = (\lambda\alpha + \gamma)^3 + (\beta + \lambda^2\gamma)^3. \tag{2.2}$$

As an example, we recover the two pairs of aforementioned taxi-cab cubes by putting $(\alpha, \beta, \gamma, \lambda) = (3, 0, 1, 3)$ in (2.2).

Although several formulations equivalent to Euler's general solution have been discovered, Ramanujan's formulation (2.2) appears to be the simplest of all. The problem of completely characterizing all positive integral solutions of (2.1) is unsolved.

On the other hand, Euler conjectured that there were no positive integral solutions to

$$A^4 + B^4 + C^4 = D^4.$$

It was not until 1988 that Euler's conjecture was shown to be false by N. D. Elkies [**9**], who found an infinite class of solutions.

Ramanujan derived several theorems providing infinite families of solutions for equal sums of powers. For example, toward the end of this third notebook [**26**, p. 384], he writes two parametric solutions for representing a fourth power as a sum of five fourth powers.

Theorem. *If s, t, m, and n are arbitrary, then*

$$(8s^2 + 40st - 24t^2)^4 + (6s^2 - 44st - 18t^2)^4 + (14s^2 - 4st - 42t^2)^4$$
$$+ (9s^2 + 27t^2)^4 + (4s^2 + 12t^2)^4 = (15s^2 + 45t^2)^4 \tag{2.3}$$

and

$$(4m^2 - 12n^2)^4 + (3m^2 + 9n^2)^4 + (2m^2 - 12mn - 6n^2)^4$$
$$+ (4m^2 + 12n^2)^4 + (2m^2 + 12mn - 6n^2)^4 = (5m^2 + 15n^2)^4. \tag{2.4}$$

Ramanujan recorded several examples. For instance, if we set $s = 1$ and $t = 0$ in (2.3), we find that

$$4^4 + 6^4 + 8^4 + 9^4 + 14^4 = 15^4.$$

Formula (2.3) is due to C. B. Haldeman [**12**, pp. 289–290] in 1904. Uncannily, Ramanujan used the same notation and recorded the terms in the same order as Haldeman! Likewise, (2.4) was established by Haldeman [**12**, p. 289] and slightly later by A. Martin [**15**, pp. 325–326, 331]. Ramanujan does not use Haldeman's notation in (2.4) but does employ Martin's notation!

Ramanujan recorded his results in notebooks from about 1903 until he departed for England in 1914. The 16 chapters in the first notebook and the 21 chapters in the second evince a progressive maturation from more elementary mathematics to much deeper results. The third notebook, however, contains both very elementary results as well as advanced results. While the latter theorems may have been recorded in Cambridge, the former results were probably recorded early in the period 1903–1914. Since in India Ramanujan did not have access to even the primary mathematical journals of his day, it is extremely unlikely that he could have seen the obscure journal, *Mathematical Magazine*, in which Martin and Haldeman published their results. Thus, the notation in (2.3) and (2.4) being identical with that of Haldeman and Martin, respectively, must be coincidental.

Mathematical Magazine was founded and edited by Martin and was devoted to "elementary mathematics." Issues of the first volume were published quarterly in

1882–1884 at a cost of 50 cents per issue or one dollar per year. The second and last volume of 12 issues was published over the years 1890–1904, with the last four issues appearing in January, 1895; January, 1896; December, 1898; and January, 1904. The last issue contains four papers, three by Martin and one by Haldeman. In the penultimate issue, under the heading "Editorial Items," we learn that "Since No. 10 of the Magazine was published, three able contributors have 'crossed over' and 'passed beyond the confines of earth.'" It is likely that an even greater number "crossed over" between the 11th and 12th issues. Possibly due to complaints registered by readers disgruntled over the irregularity at which issues appeared, the price per issue had dropped to 30 cents.

Toward the end of the third notebook [**26**, p. 386], Ramanujan records one of the most fascinating identities we have ever seen.

Theorem. *Let a, b, c, and d denote any numbers such that $ad = bc$. Then*

$$\begin{aligned}
&64\{(a+b+c)^6 + (b+c+d)^6 - (c+d+a)^6 - (d+a+b)^6 \\
&\qquad\qquad + (a-d)^6 - (b-c)^6\} \\
&\times\{(a+b+c)^{10} + (b+c+d)^{10} - (c+d+a)^{10} - (d+a+b)^{10} \\
&\qquad\qquad + (a-d)^{10} - (b-c)^{10}\} \\
&= 45\{(a+b+c)^8 + (b+c+d)^8 - (c+d+a)^8 - (d+a+b)^8 \\
&\qquad\qquad + (a-d)^8 - (b-c)^8\}^2. \qquad (2.5)
\end{aligned}$$

The hypothesis $ad = bc$ was omitted by Ramanujan, although it does appear as a hypothesis for some related results on the previous page.

We first transcribe (2.5) into a somewhat more transparent form. For each positive integer m, set

$$\begin{aligned}
F_{2m}(a,b,c,d) &= (a+b+c)^{2m} + (b+c+d)^{2m} - (c+d+a)^{2m} \\
&\quad - (d+a+b)^{2m} + (a-d)^{2m} - (b-c)^{2m}.
\end{aligned}$$

Put $b = ax$, $c = ay$, and $d = axy$, which does not contravene the hypothesis $ad = bc$. Then it is easy to see that

$$F_{2m}(a,b,c,d) = a^{2m} f_{2m}(x,y),$$

where

$$\begin{aligned}
f_{2m}(x,y) &= (1+x+y)^{2m} + (x+y+xy)^{2m} - (y+xy+1)^{2m} \\
&\quad - (xy+1+x)^{2m} + (1-xy)^{2m} - (x-y)^{2m}. \qquad (2.6)
\end{aligned}$$

Hence, (2.5) can be put in the form

$$64 f_6(x,y) f_{10}(x,y) = 45 f_8^2(x,y). \qquad (2.7)$$

We first employed the computer algebra system *Mathematica* to verify (2.7). Next, using Mathematica, we attempted to find other identities like (2.7) involving $f_{2m}(x,y)$ for $m \le 10$, but we were unsuccessful. We fortunately found a much more informative proof of (2.7) that is not merely a verification via computer algebra [**6**]. We will not repeat that proof here but instead offer a few additional remarks.

By inspection, we easily see that $x = 0, 1, -1, -2, -1/2$ are zeros of $f_{2m}(x, y)$. By symmetry, $y = 0, 1, -1, -2, -1/2$ are also zeros. Since f_{2m} has degree (at most) $2m$ in each of the variables x and y, it follows that $f_2(x, y) \equiv 0 \equiv f_4(x, y)$. In our original notation, we have therefore proved that, if $ad = bc$, then

$$(a+b+c)^n + (b+c+d)^n + (a-d)^n = (c+d+a)^n + (d+a+b)^n + (b-c)^n, \tag{2.8}$$

where $n = 2$ or 4. These are the aforementioned results that appear on page 385 of [**26**]. We have therefore returned to the problem of generating equal sums of biquadrates. Although many results have appeared in the literature yielding two equal sums of three biquadrates [**8**, pp. 653–657], none appear as simple as Ramanujan's identity (2.8).

Are (2.5) and (2.7) merely accidents, or are they a manifestation of some far deeper theorem?

3. ELEMENTARY ALGEBRA. In courses and texts on beginning calculus, students encounter many monotonic sequences in their study of sequences and series. An inquisitive student may ask for naturally occurring examples of sequences that increase for a while, then decrease for a while, etc. As we shall see, some infinite sequences of nested radicals of Ramanujan provide excellent examples.

Mrs. Ramanujan (S. Janaki Ammal) and W. Narayanan, one of her two adopted sons.

In 1914, Ramanujan [**22**], [**27**, pp. 327–329] posed the following problem to readers of the *Journal of the Indian Mathematical Society*: Solve completely

$$x^2 = y + a, \qquad y^2 = z + a, \quad \text{and} \quad z^2 = x + a. \tag{3.1}$$

Concomitantly, he asked for the evaluation of three infinite sequences of nested radicals. Toward the end of his second notebook [**26**, pp. 305–307], Ramanujan recorded further and more general results. It is not difficult to see that x is a root of an octic polynomial. This polynomial can be factored over the quadratic field

$Q(\sqrt{4a-7})$ into one quadratic and two cubic factors. These factors are correctly given by Ramanujan in his solution [**22**], but the factors given in the solution printed in his *Collected Papers* [**27**, pp. 327–329] contain four sign errors.

From the equalities (3.1), we find that

$$x = \sqrt{a+y} = \sqrt{a+\sqrt{a+z}} = \sqrt{a+\sqrt{a+\sqrt{a+x}}}$$
$$= \sqrt{a+\sqrt{a+\sqrt{a+\sqrt{a+\cdots}}}}\,. \tag{3.2}$$

Each square root should be considered two-valued, and so we are led to eight infinite sequences of nested radicals corresponding to the eight roots of our octic polynomial. First, we should determine those values of a for which the infinite radical in (3.2) converges. This is not an easy problem, but each of the eight sequences in (3.2) converges at least for $a \geq 2$ [**5**, Chapter 22]. As a specific example, let

$$a_1 = \sqrt{a}, \qquad a_2 = \sqrt{a-\sqrt{a}}, \qquad a_3 = \sqrt{a-\sqrt{a+\sqrt{a}}},$$
$$a_4 = \sqrt{a-\sqrt{a+\sqrt{a+\sqrt{a}}}}, \ldots,$$

where the sequence of signs $-, +, +, \ldots$ appearing in the nested radicals has period 3. A careful analysis shows that

$$a_{6n+1} > a_{6n+2} > a_{6n+3} > a_{6n+4}$$

and

$$a_{6n+4} < a_{6n+5} < a_{6n+6} < a_{6n+7},$$

for each nonnegative integer n. Furthermore,

$$0 < a_4 < a_{10} < \cdots < a_{6n+4} < a_{6n+7} < a_{6n+1} < \cdots < a_7 < a_1 = \sqrt{a}\,.$$

Thus, $\{a_{6n+1}\}$ and $\{a_{6n+4}\}$ converge. Next, it must be shown that $\{a_{3n+1}\}$ converges and, lastly, that $\{a_n\}$ converges. The details in this analysis are not easy [**5**, Chapter 22].

If we solve the two cubic equations mentioned above, it is not easy, in general, to identify the roots with the appropriate infinite sequences of radicals. For example,

$$\lim_{n\to\infty} a_n = \frac{A-1}{6} + \frac{2}{3}\sqrt{4a+A}\,\sin\left(\frac{1}{3}\arctan\frac{2A+1}{3\sqrt{3}}\right), \tag{3.3}$$

where $A = \sqrt{4a-7}$. We made these identifications by expanding both the algebraically determined roots and the infinite radicals around "$a = \infty$." For example, both sides of (3.3) have the asymptotic expansions

$$\sqrt{a} - \frac{1}{2} - \frac{3}{8\sqrt{a}} - \frac{1}{4a} + \cdots,$$

as a tends to ∞. For particular numerical examples, the proper identifications are easier to make. For instance, if $a = 2$ in (3.3),

$$2\sin\left(\frac{\pi}{18}\right) = \sqrt{2-\sqrt{2+\sqrt{2+\sqrt{2-\cdots}}}}\,.$$

Later, Ramanujan [25], [27, p. 332] submitted the similar problem of determining the simultaneous solutions of the system,

$$x^2 = a + y, \qquad y^2 = a + z, \qquad z^2 = a + u, \quad \text{and} \quad u^2 = a + x,$$

to the *Journal of the Indian Mathematical Society*. Fourteen years elapsed before a solution by G. N. Watson [29] was published, while another solution can be found in [5, Chapter 22]. As above, interesting sequences of nested radicals arise. For example,

$$\frac{1}{2}\left(2 + \sqrt{5} + \sqrt{15 - 6\sqrt{5}}\right) = \sqrt{5 + \sqrt{5 + \sqrt{5 - \sqrt{5 + \sqrt{5 + \cdots}}}}},$$

where the infinite sequence of signs $+, +, -, +, \cdots$ has period 4.

The theory of infinite sequences of nested radicals has not been well developed, probably because general theorems are difficult to obtain and convergence is slow. For further examples, theorems, and references to the literature, see [3, pp. 108–112] and [5, Chapter 22].

In the unorganized portions of his notebooks [26] and in the problem sections of the *Journal of the Indian Mathematical Society*, Ramanujan offers other problems on systems of equations. Thus, on page 338 of [26], he asks for the solutions of

$$\frac{x^5 - a}{x^2 - y} = \frac{y^5 - b}{y^2 - x} = 5(xy - 1),$$

where a and b are arbitrary constants. There are 25 pairs (x, y) of solutions. The special case $a = 6$, $b = 9$ appeared as Question 284 [20], [27, pp. 322–323] in the *Journal of the Indian Mathematical Society*. Ramanujan's solution was the only one received, and a similar solution to the more general problem can be found in [5, Chapter 22].

Question 284 was the fourth problem that Ramanujan published in the *Journal of the Indian Mathematical Society*. The first five problems that Ramanujan posed to *Journal* readers were published under the name S. Ramanujam. Ramanujan and Ramanujam are two versions of the same Sanskrit name RAMANUJAHA, which means younger brother of Rama.

We mention one further system of equations studied by Ramanujan. On page 338 of his second notebook, Ramanujan asks, in slightly different notation, for the solutions of the system of $2n$ equations,

$$x_1 y_1^{j-1} + x_2 y_2^{j-1} + \cdots + x_n y_n^{j-1} = a_j, \qquad 1 \le j \le 2n, \tag{3.4}$$

where $x_1, \ldots, x_n, y_1, \ldots, y_n$ are $2n$ unknowns, and in his short paper [21], [27, pp. 18–19], Ramanujan presents his clever solution, which we briefly indicate.

Ramanujan defines

$$\varphi(\theta) := \sum_{j=1}^{n} \frac{x_j}{1 - \theta y_j}. \tag{3.5}$$

When $\varphi(\theta)$ is expanded in a power series in θ, it is seen that the coefficient of θ^k is a_{k+1}, $0 \le k \le 2n - 1$. On the other hand, $\varphi(\theta)$ has the form

$$\varphi(\theta) = \frac{\sum_{j=0}^{n-1} A_{j+1}\theta^j}{1 + \sum_{j=1}^{n} B_j\theta^j}. \tag{3.6}$$

Clearing the denominator in (3.6) and using the aforementioned power series for $\varphi(\theta)$, we can determine first the coefficients B_j, $1 \le j \le n$, and secondly the

coefficients A_j, $1 \le j \le n$, in terms of $a_1, a_2, \ldots, a_{2n}$ by equating coefficients of like powers of θ. Having explicitly determined A_j and B_j, $1 \le j \le n$, we substitute these values into (3.6) and once again expand $\varphi(\theta)$ into partial fractions. Comparing the result with (3.5), we determine x_j and y_j, $1 \le j \le n$.

It is easy to see that the system (3.4) is equivalent to the single equation

$$\sum_{i=1}^{n} x_i (y_i s + t)^{2n-1} = \sum_{j=0}^{2n-1} \binom{2n-1}{j} a_{j+1} s^j t^{2n-1-j}.$$

Thus, Ramanujan's query is equivalent to the question: When can a binary $(2n-1)-ic$ form be represented as a sum of n $(2n-1)th$ powers? In 1851, Sylvester [**28**, pp. 203–216, 265–283] found the following necessary and sufficient conditions for a solution: The system of n equations

$$a_j u_1 + a_{j+1} u_2 + \cdots + a_{j+n} u_{n+1} = 0, \qquad 1 \le j \le n,$$

must have a solution $u_1, u_2, \ldots, u_{n+1}$ such that the $n-ic$ form

$$p(w, z) := \sum_{j=0}^{n} u_{j+1} w^j z^{n-j}$$

can be represented as a product of n distinct linear forms. This is true for a general $2n$-tuple $(a_1, a_2, \ldots, a_{2n})$ in the sense of algebraic geometry. Thus, the numbers $y_1, y_2, \ldots, y_n$ are related to the factorization of $p(w, z)$. Sylvester's theorem belongs to the subject of invariant theory, which was developed in the late 19th and early 20th centuries. For a contemporary treatment, but with classical language, see a paper by J. P. S. Kung and G.-C. Rota [**14**].

We next consider the following theorem of Ramanujan [**26**, p. 325].

Theorem. *Let α, β, and γ denote the roots of the cubic equation*

$$x^3 - ax^2 + bx - 1 = 0. \tag{3.7}$$

Then, for a suitable determination of roots,

$$\alpha^{1/3} + \beta^{1/3} + \gamma^{1/3} = (a + 6 + 3t)^{1/3} \tag{3.8}$$

and

$$(\alpha\beta)^{1/3} + (\beta\gamma)^{1/3} + (\gamma\alpha)^{1/3} = (b + 6 + 3t)^{1/3}, \tag{3.9}$$

where

$$t^3 - 3(a + b + 3)t - (ab + 6(a + b) + 9) = 0. \tag{3.10}$$

Since this beautiful elementary theorem is evidently new and since a short proof can be given, we provide one here.

Proof: Noting, from (3.7), that $\alpha\beta\gamma = 1$, let

$$z^3 - \theta z^2 + \varphi z - 1 = 0 \tag{3.11}$$

denote the cubic polynomial with roots $\alpha^{1/3}$, $\beta^{1/3}$, and $\gamma^{1/3}$, chosen so that their product equals 1. Cubing both sides of the equality

$$z^3 - 1 = \theta z^2 - \varphi z,$$

we find that

$$(z^3 - 1)^3 - \theta^3 z^6 + \varphi^3 z^3 + 3\theta\varphi z^3 (z^3 - 1) = 0. \tag{3.12}$$

Since $\alpha^{1/3}$, $\beta^{1/3}$, and $\gamma^{1/3}$ are roots of (3.11), they are also roots of (3.12). As a cubic polynomial in z^3, (3.12) thus has the roots α, β, and γ.

Comparing (3.7) and (3.12), we deduce that

$$a = \theta^3 + 3 - 3\theta\varphi \tag{3.13}$$

and

$$b = \varphi^3 + 3 - 3\theta\varphi. \tag{3.14}$$

If we define t by

$$\theta^3 = a + 6 + 3t, \tag{3.15}$$

then, by (3.11) and (3.15),

$$\alpha^{1/3} + \beta^{1/3} + \gamma^{1/3} = \theta = (a + 6 + 3t)^{1/3},$$

which proves (3.8). Also, by (3.13)–(3.15),

$$\varphi^3 = b - 3 + 3\theta\varphi = b + \theta^3 - a = b + 6 + 3t. \tag{3.16}$$

Hence, by (3.11) and (3.16), (3.9) is established. From (3.13) and (3.15),

$$3 + t = \theta\varphi. \tag{3.17}$$

Thus, by (3.15)–(3.17),

$$(3 + t)^3 = \theta^3\varphi^3 = (a + 6 + 3t)(b + 6 + 3t).$$

Expanding both sides, collecting terms, and simplifying, we deduce (3.10).

On page 356 of [**26**], the last page of the second notebook, Ramanujan offers the equalities

$$\left(\cos\frac{2\pi}{9}\right)^{1/3} + \left(\cos\frac{4\pi}{9}\right)^{1/3} - \left(\cos\frac{\pi}{9}\right)^{1/3} = \left\{\frac{3}{2}(9^{1/3} - 2)\right\}^{1/3} \tag{3.18}$$

and

$$\left(\sec\frac{2\pi}{9}\right)^{1/3} + \left(\sec\frac{4\pi}{9}\right)^{1/3} - \left(\sec\frac{\pi}{9}\right)^{1/3} = \{6(9^{1/3} - 1)\}^{1/3}, \tag{3.19}$$

which are applications of (3.8) and (3.9), respectively, with $a = 0$, $b = -3$, and $t = -9^{\frac{1}{3}}$. Equality (3.18) was posed as a problem by Ramanujan in the *Journal of the Indian Mathematical Society* [**23**], [**27**, p. 329]. Proofs of (3.18) and (3.19) can also be found in Berndt's book [**5**, Chapter 22].

4. NUMBER THEORY. Suppose p is a prime and n is a positive integer. Then, by a well-known theorem in elementary number theory [**19**, p. 182], the highest power of p dividing $n!$ equals

$$\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] =: N.$$

Despite the widespread use of this theorem by number theorists for many years, the inequalities

$$\frac{n}{p-1} - \frac{\log(n+1)}{\log p} \le N \le \frac{n-1}{p-1}, \tag{4.1}$$

given by Ramanujan [**26**, p. 378] in his third notebook do not appear to have been heretofore noticed. Both inequalities in (4.1) are sharp. If $n = p^m$ for some positive integer m, an elementary calculation shows that $N = (n-1)/(p-1)$.

On the other hand, if $n = p^{m+1} - 1$, by a direct calculation with the observation that $m + 1 = \log(n + 1)/\log p$,

$$N = \frac{n}{p-1} - \frac{\log(n+1)}{\log p}.$$

In fact, Ramanujan stated (4.1) with p replaced by an arbitrary positive integer $a \geq 2$.

Bhargava, Adiga, and Somashekara [7] have given one proof of (4.1) when p is any positive integer exceeding 1. We offer another proof here.

Proof of (4.1): First, by writing n in base p, i.e., by setting

$$n = \sum_{j=0}^{m} b_j p^j, \qquad 0 \leq b_j \leq p - 1, \quad b_m \neq 0,$$

we find, after a straightforward calculation, that

$$N = \frac{n}{p-1} - \frac{1}{p-1}\sum_{j=0}^{m} b_j, \tag{4.2}$$

and so the second inequality in (4.1) follows.

The first inequality in (4.1) is more difficult to establish. We are very grateful to B. Reznick for supplying the following elegant proof.

Set

$$b = \sum_{j=0}^{m} b_j.$$

Then, by (4.2), it suffices to prove that

$$b \leq (p-1)\frac{\log(n+1)}{\log p}. \tag{4.3}$$

Write

$$b = k(p-1) + r, \qquad 0 \leq r \leq p - 2. \tag{4.4}$$

Then

$$\begin{aligned} n &\geq (p-1)p^0 + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^{k-1} + rp^k \\ &= (r+1)p^k - 1. \end{aligned}$$

It follows that

$$\begin{aligned} (p-1)\frac{\log(n+1)}{\log p} &\geq (p-1)\frac{\log((r+1)p^k)}{\log p} \\ &= k(p-1) + (p-1)\frac{\log(r+1)}{\log p}. \end{aligned} \tag{4.5}$$

By (4.3)–(4.5), we shall be finished with the proof if we can show that

$$r \leq (p-1)\frac{\log(r+1)}{\log p}. \tag{4.6}$$

First, if $r = 0$, (4.6) clearly holds with equality.

If $r \geq 1$, (4.6) can be written in the form

$$\frac{r}{\log(r+1)} \leq \frac{p-1}{\log p},$$

or

$$f(r) \leq f(p-1), \tag{4.7}$$

where

$$f(x) := \frac{x}{\log(x+1)}.$$

However, by elementary calculus, $f(x)$ is strictly increasing for positive integral x. Since $1 \leq r \leq p-2$, (4.7) is therefore valid with a strict inequality, and so the proof is complete.

As remarked in the Introduction, we conclude this short sampling of Ramanujan's elementary discoveries with a note on π. Continued fractions provide excellent rational approximations to π. Thus, the simple continued fraction

$$\pi = 3 + \frac{1}{7} + \frac{1}{15} + \frac{1}{1} + \frac{1}{293} + \cdots$$

yields the successive approximations $\frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \ldots$. Note that

$$\frac{355}{113} = 3.14159\,29\ldots,$$

which agrees with the decimal expansion of $\pi = 3.14159\,26535\ldots$ through 6 decimal places. The appearance of a "large" fourth partial quotient, 293, is primarily responsible for this success.

Taking a brief diversion in his famous paper on approximations to π [**24**], [**27**, p. 35], Ramanujan offers the approximation

$$\pi \approx \left(97\frac{1}{2} - \frac{1}{11}\right)^{1/4} = 3.14159\,26526\ldots, \tag{4.8}$$

which "was obtained empirically." How did Ramanujan deduce this unusual approximation, which is also found in his second and third notebooks [**26**, pp. 217, 375]? N. D. Mermin [**16**], [**17**, pp. 304–305] has offered the best explanation for Ramanujan's approximation (4.8). In the decimal expansion of $\pi^4 = 97.409091034002\ldots$, observe that the pair of digits 09 appears twice in succession followed by the pair 10, which is 'close' to 09. Thus,

$$97.40909090909\ldots = \frac{2143}{22} = 97\frac{1}{2} - \frac{1}{11}$$

is a natural approximation to π^4.

Ramanujan's facility with continued fractions is unequaled in mathematical history, and so he might have observed that [**16**], [**17**], [**4**, p. 151]

$$\pi^4 = 97 + \frac{1}{2} + \frac{1}{2} + \frac{1}{3} + \frac{1}{1} + \frac{1}{16539} + \frac{1}{1} + \cdots.$$

Truncating this continued fraction just before the "super large" partial quotient 16,539 gives the approximation (4.8).

We are very grateful to Richard Askey, R. William Gosper, Daniel Grayson, K. Srinivasa Rao, and Bruce Reznick for valuable contributions.

REFERENCES

1. G. E. Andrews, R. A. Askey, B. C. Berndt, K. G. Ramanathan, and R. A. Rankin, editors, *Ramanujan Revisited*, Academic Press, Boston, 1988.
2. E. T. Bell, *The Last Problem*, Mathematical Association of America, Washington, D.C., 1990.
3. B. C. Berndt, *Ramanujan's Notebooks, Part II*, Springer-Verlag, New York, 1989.
4. ______, *Ramanujan's Notebooks, Part III*, Springer-Verlag, New York, 1991.
5. ______, *Ramanujan's Notebooks, Part IV*, Springer-Verlag, New York, 1994.
6. B. C. Berndt and S. Bhargava, A remarkable identity found in Ramanujan's third notebook, *Glasgow Math. J.* 34 (1992), 341–345.
7. S. Bhargava, C. Adiga, and D. D. Somashekara, An estimate of Ramanujan related to the greatest integer function, *Bull. Austral. Math. Soc.* 44 (1991), 149–154.
8. L. E. Dickson, *History of the Theory of Numbers*, vol. 2, Chelsea, New York, 1966.
9. N. D. Elkies, On $A^4 + B^4 + C^4 = D^4$, *Math. of Comp.* 51 (1988), 825–835.
10. L. Euler, *Solutio generalis quorundam problematum diophanteorum quae vulgo nonnise solutiones speciales admittere videntur*, Opera Omnia, Ser. I, vol. 2, B. G. Teubner, Lipsiae, 1915, pp. 428–458.
11. P. Fermat, *Oeuvres*, t. 3, Gauthier-Villars, Paris, 1896.
12. C. B. Haldeman, On biquadrate numbers, *The Mathematical Mag.* 2 (1904), 285–296.
13. G. H. Hardy, *Ramanujan*, 3rd edition, Chelsea, New York, 1978.
14. J. P. S. Kung and G.-C. Rota, The invariant theory of binary forms, *Bull. Amer. Math. Soc.* 10 (1984), 27–85.
15. A. Martin, About biquadrate numbers whose sum is a biquadrate-II, *The Mathematical Mag.* 2 (1904), 325–362.
16. N. D. Mermin, Pi in the sky, *Am. J. Phys.* 55 (1987), 584–585.
17. ______, *Boojums All the Way Through*, Cambridge University Press, Cambridge, 1990.
18. C. Moreau, Plus petit nombre égal à la somme de deux cubes de deux facons, *L'Intermediaire Math.* 5 (1898), 66.
19. I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.
20. S. Ramanujan, Question 284, *J. Indian Math. Soc.* 4 (1912), 183.
21. ______, Note on a set of simultaneous equations, *J. Indian Math. Soc.* 4 (1912), 94–96.
22. ______, Question 507, *J. Indian Math. Soc.* 6 (1914), 74–77.
23. ______, Question 524, *J. Indian Math. Soc.* 6 (1914), 190–191.
24. ______, Modular equations and approximations to π, *Quart. J. Math.* (Oxford) 45 (1914), 350–372.
25. ______, Question 722, *J. Indian Math. Soc.* 7 (1915), 240.
26. ______, *Notebooks* (2 volumes), Tata Institute of Fundamental Research, Bombay, 1957.
27. ______, *Collected Papers*, Chelsea, New York, 1962.
28. J. J. Sylvester, *Collected Mathematical Papers*, vol. 1, Chelsea, New York, 1973.
29. G. N. Watson, Solution to Question 722, *J. Indian Math. Soc.* 18 (1929), 113–117.
30. ______, Ramanujan's note books, *J. London Math. Soc.* 6 (1931), 137–153.

Department of Mathematics
University of Illinois
Urbana, IL 61801

Department of Mathematics
University of Mysore
Manasa Gangotri
Mysore 570 006, India

Chebychev Polynomials and Regular Polygons

D. Y. Savio and E. R. Suryanarayan

1. INTRODUCTION. Chebychev polynomials occur in many branches of mathematics: interpolation theory, orthogonal polynomials, approximation theory, numerical analysis, ergodic theory, etc. It is said that the Chebychev polynomial is like a fine jewel that reveals its different characteristics under illumination from varying positions [**2**]. There is yet a simple spot it shows its radiance: Regular Polygons. In this paper we study some of the properties of the Chebychev polygons of the second kind $u_n(x)$, (2) below, and a polynomial associated with it, namely, $u_n + u_{n-1}$ and learn that the polynomials are related to some of the properties of the regular polygons. Specifically, we generalize a result due to Kepler (1571–1630). Kepler observed that the squares of the edges of polygons $\{7\}$, $\left\{\begin{smallmatrix}7\\2\end{smallmatrix}\right\}$, $\left\{\begin{smallmatrix}7\\3\end{smallmatrix}\right\}$ of unit circumradius (all having the same 7 vertices) are the roots of the equation,

$$z^3 - 7z^2 + 14z^2 - 7 = 0; \tag{1}$$

here, $\{7\}$ is a regular heptagon; $\left\{\begin{smallmatrix}7\\2\end{smallmatrix}\right\}$ and $\left\{\begin{smallmatrix}7\\3\end{smallmatrix}\right\}$ are star-polygons [**1**] (see FIGURE 1).

2. CHEBYCHEV POLYNOMIALS. Let $x = \cos\theta$. Chebychev polynomials of the second kind are defined recursively by [**2**], $u_n(x)$:

$$u_0(x) = 1, \qquad u_1(x) = 2x, \dots, u_n(x) = \frac{\sin(n+1)\theta}{\sin\theta}, \qquad n = 1, 2, \dots. \tag{2}$$

$u_n(x)$ satisfies the classical recurrence

$$u_n(x) = 2xu_{n-1} - u_{n-2}. \tag{3}$$

The zeros of $u_n(x)$ are

$$\cos\frac{k\pi}{n+1}, \qquad k = 1, \dots, n \tag{4}$$

[**2**]. We need the following result for later use.

Theorem 1. *Let $v_n(x) = u_n(x) + u_{n-1}(x)$. Then the zeros of $v_n(x)$ are* $\cos(2k\pi/2n+1)$.

Proof: From the trigonometric definition of u_n and elementary trigonometric identities, we find that $v_n = (\sin(n+\frac{1}{2})\theta/\sin(\theta/2))$. Therefore, the zeros of $v_n(x)$ are $\cos(2k\pi/2n+1)$. ∎

Let

$$U_n(x) = \begin{bmatrix} 2x & 1 & 0 & 0 & \cdots & 0 \\ 1 & 2x & 1 & 0 & \cdots & 0 \\ 0 & 1 & 2x & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 & 2x \end{bmatrix}, \tag{5}$$

where the matrix is symmetric, tridiagonal and is of order n. The result

$$u_n(x) = \operatorname{Det} U_n(x) \tag{6}$$

follows from the recurrence (3) [**3**].

Theorem 2. *The eigenvalues of* $U_n(x)$ *are* $2(x-1) + 4\sin^2(k\pi/2n+2)$, $k = 1, 2, \ldots, n$.

Proof: From (6) the eigenvalues of U_n are the zeros of $u_n(x - (\lambda/2))$; but from (4) the zeros of $u_n(x - (\lambda/2))$ are given $2x - 2\cos(k\pi/n + 1)$. Therefore, the eigenvalues of U_n are $2(x-1) + 4\sin^2(k\pi/2n+2)$. ■

There is a pair of recurrences less well known which also generates u_n:

$$u_{2n} = (u_n + u_{n+1})(u_{n+1} - u_{n-1}), \tag{7}$$

$$u_{2n+1} = u_n(u_{n+1} - u_{n-1}), \qquad n = 1, 2, \ldots \tag{8}$$

The preceding "odd-even" breakdown can be proved by using the definition (2) and elementary trigonometric identities. The above relations suggest that u_n is always the product of two determinants which are themselves "Chebychev polynomials" in the sense of $u_k \pm u_{k-1}$ and $u_{k+1} - u_{k-1}$ satisfy recurrence (3). Indeed,

$$u_k \pm u_{k-1} = 2xu_{k-1} - u_{k-2} \pm u_{k-1} = (2x \pm 1)u_{k-1} - u_{k-2}$$

$$= \operatorname{Det} \begin{bmatrix} 2x & 1 & 0 & 0 & \cdots & 0 \\ 1 & 2x & 1 & 0 & \cdots & 0 \\ 0 & 1 & 2x & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 & 2x \pm 1 \end{bmatrix} \tag{9}$$

and

$$u_{k+1} - u_{k-1} = 2xu_k - 2u_{k-1} = \operatorname{Det} \begin{bmatrix} 2x & 1 & 0 & 0 & \cdots & 0 \\ 1 & 2x & 1 & 0 & \cdots & 0 \\ 0 & 1 & 2x & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 2 & 2x \end{bmatrix} \tag{10}$$

differ from (5) just at a single entry.

When $n = 2k + 1$, let

$$V_n = \begin{bmatrix} 2x & 1 & 0 & 0 & \cdots & 0 \\ 1 & 2x & 1 & 0 & \cdots & 0 \\ 0 & 1 & 2x & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 & 2x + 1 \end{bmatrix}, \qquad n = 1, 3, 5, \ldots \tag{11}$$

denote the square matrix of order k. When $n = 2k$, let U_n be defined by (5). All statements with U_n and V_n assume $n = 2k$ and $n = 2k + 1$ respectively.

Theorem 3. *The eigenvalues of* $V_n(x)$ *are* $2(x - 1) + 4\sin^2(k\pi/2n + 1)$, $k = 1, 2, \ldots, n$.

Proof: The eigenvalues of V_n are obtained by solving the equation $\operatorname{Det} V_n(2(x - \lambda/2)) = 0$, for λ. Since $\operatorname{Det} V_n = v_n$ and the zeros of $v_n(x - (\lambda/2))$ are $2(x - 1) + 4\sin^2(k\pi/2n + 1)$, we see, from an argument similar to theorem 1, that the zeros of $v_n(x - (\lambda/2))$ are indeed the eigenvalues of V_n. ■

3. APPLICATION TO REGULAR STAR-FIGURES AND POLYGONS. A *regular star-figure* is a figure formed by connecting with straight lines every qth point, starting with one of the points that divide a circumference into n equal parts ($2q < n$); if all the n points are not connected, then start from the unconnected point next to the initial point, and repeat the connecting procedure until all the n points are connected. Such a star-figure is denoted by $\left\{ {n \atop q} \right\}$. If $q = 1$, we have a regular convex polygon $\{n\}$ of n sides. If n and q are relatively prime, the star-figure is a star-polygon or an n-gram. For a given n there are $\phi(n)/2$ regular n-grams where $\phi(n)$ is the Euler function, the number of numbers less than n and prime to it. If n and q are not relatively prime then $\left\{ {n \atop q} \right\}$ is a symmetrically superposed convex polygon. For example, $\left\{ {5 \atop 2} \right\}$ is a pentagram, whereas, the star-figure $\left\{ {6 \atop 2} \right\}$ (the star of David) is formed by two equilateral triangles symmetrically superposed.

Regular octagons and 16-gons occur in the mural decorations of ancient Egypt. Pentagrams and hexagons were used by the Babylonians. Pythagoreans used pentagram as a symbol of good health and also as a badge of recognition. Hindus use the star of Lakshmi $\left\{ {8 \atop 2} \right\}$ to symbolize the eight forms of wealth (*Ashtalakshmi*). Buddhists and Hindus draw, an elaborate form of star-figures and star-polygons, a *mandala*, on the ceremonial altars. The systematic study of the star-polygons was initiated and some of their properties were developed by Bradwardine (1290–1349), an English cleric who became Archbishop of Canterbury for the last month of his life.

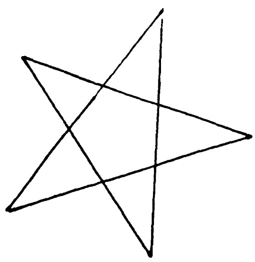
Consider a regular star-figure of n sides. Let O be the center, M the mid-point and A one end of the side, and let AM $= (l/2)$ and OA $= R$ be the circumradius of the star-figure (Figure 2). The angle AOM is π/n for $\{n\}$ and $q\pi/n$ for the star-figure $\left\{ {n \atop q} \right\}$ and the edges are $2R\sin(\pi/2n)$ and $2R\sin(q\pi/2n)$ respectively.

From the above results and theorems 2 and 3, we have the following generalization of Kepler's observation:

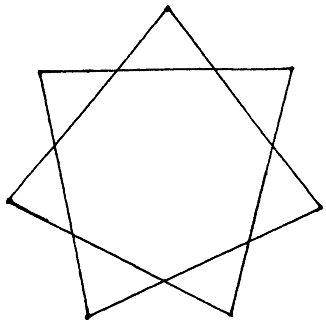
Theorem 4. *Let l be an edge and R the circumradius of a regular star-figure of n sides. The eigenvalues of the matrices $V_n(1)$ and $U_n(1)$ are the ratios $(l/R)^2$ of the regular star-figures $\left\{ {n \atop j} \right\}$, $j = 1, 2, \ldots, k$, if $n = 2k + 1$, and $j = 1, 2, \ldots, k - 1$, if $n = 2k$.*

As a special case, consider the characteristic equation of $V_3(1)$:

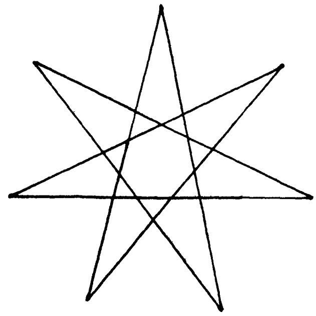
$$\begin{bmatrix} 2-\lambda & 1 & 0 \\ 1 & 2-\lambda & 1 \\ 0 & 1 & 3-\lambda \end{bmatrix} = 0.$$



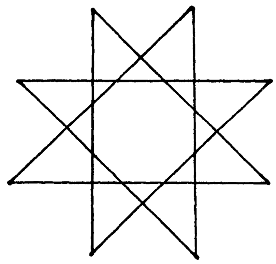
(a) $\begin{Bmatrix} 5 \\ 2 \end{Bmatrix}$



(b) $\begin{Bmatrix} 7 \\ 2 \end{Bmatrix}$

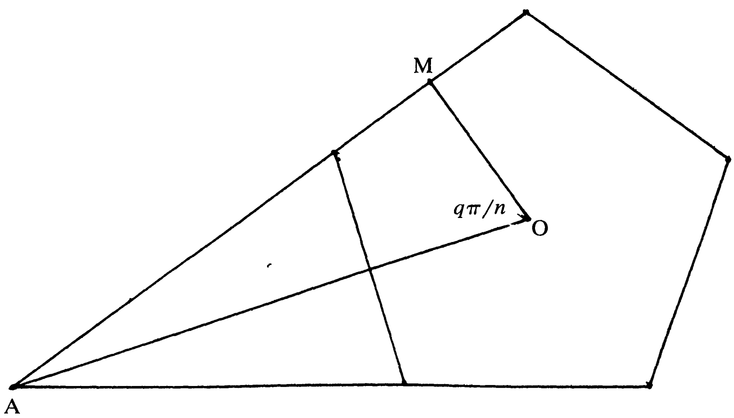


(c) $\begin{Bmatrix} 7 \\ 3 \end{Bmatrix}$



$\begin{Bmatrix} 8 \\ 3 \end{Bmatrix}$

Figure 1



$\begin{Bmatrix} n \\ q \end{Bmatrix}$

Figure 2

On expansion, the above equation reduces to $\lambda^3 - 7\lambda^2 + 14\lambda - 7 = 0$. Similarly, the three roots of the characteristic equation of $U_3(1)$:

$$\begin{bmatrix} 2-\lambda & 1 & 0 \\ 1 & 2-\lambda & 1 \\ 0 & 1 & 2-\lambda \end{bmatrix} = 0,$$

give $(l/R)^2$ for $\{8\}$, $\left\{ {8 \atop 2} \right\}$, $\left\{ {8 \atop 3} \right\}$.

REFERENCES

1. H. S. M. Coxeter, *Regular Complex Polytopes*, Cambridge U. Press, 1974, p. 8.
2. T. J. Rivlin, *The Chebychev Polynomials*, John Wiley, New York.
3. R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge U. Press, 1985, p. 28.

Department of Mathematics
University of Rhode Island
Kingston, RI 02881

PICTURE PUZZLE

(from the collection of Paul Halmos)

A teacher's teacher---one of the greatest.
(see page 697.)

Small-Group Learning

Julian Weissglass

In any math class I've been in before, I just sat and listened to a teacher talk about what was in the book and what would be assigned for homework. When I got to college the same thing was happening except here I take notes on what the professor says. I have never felt in any of these situations that I should express my opinion on the subject. The most any teacher has done to stimulate a discussion on the topic was to simply say 'Questions?' Whenever the teacher said this, though, it didn't sound like he wanted a reply.

Junior Mathematics Major

In a span of less than two years, three national reports [**6**, **9**, **10**] have recommended fundamental changes in the teaching of college mathematics. The most recent document *Moving Beyond Myths* [**10**] states, for example, that "It is widely recognized that lectures place students in a passive role, failing to engage them in their own learning. Even students who survive such courses often absorb a very misleading impression of mathematics—as a collection of skills with no connection to critical reasoning" (p. 24). The document recommends that faculty, among other things, "explore effective alternatives to 'lecture and listen'", "involve students actively in the learning process," and "teach future teachers in the ways they will be expected to teach" (p. 34).

If we take seriously the charge to "teach future teachers in the ways they will be expected to teach," a reading of the *Professional Standards for Teaching Mathematics* [**8**] (which is referred to in *Moving Beyond Myths*) will lead to using small group approaches for at least part of the class time. This document states, "Students learning of mathematics is enhanced in a learning environment that is built as a community of people collaborating to make sense of mathematical ideas. It is a key function of the teacher to develop and nurture students abilities to learn with and from others—to clarify definitions and terms to one another, consider one another's ideas and solutions, and argue together about the validity of alternative approaches and answers..." (p. 58).

Reports and recommendations, of course, do not make changes in the classroom. Only teachers doing things differently achieve that. Changing teaching, however, is not easy. There is both *individual and institutional resistance* to change. My own experience with resistance occurred during my first attempt to use a small group approach in a linear algebra class I taught in 1970, my third year as a faculty member. Although the students liked the class I was so afraid that my colleagues would find out what I was doing that I closed the door of the classroom in case any of them walked by. My anxiety caused me to abandon the approach for three years.

At the institutional level, it was not until 1991 that the MAA annual meeting provided a special session devoted to alternatives to the lecture method, although articles [**3**, **11**] appeared in the 70's describing this approach in mathematics courses and an increasing number of studies (see [**4**] for references) showed the effectiveness of small group cooperative learning approaches.

Having overcome, to some degree, my own resistance to pedagogical change, I thought it would be helpful to offer some suggestions to faculty considering

implementing small group approaches. In a sense, this is the article I wish I had been able to read twenty years ago.

BEGINNING. Do not be afraid to start slowly. It is not necessary to abandon lecturing completely. For some purposes it is a good method. You can combine lecturing, students working in groups, and whole-class discussion in any proportion you desire. One way to start is to have students form a group or pair and discuss how they solved a homework problem. Alternatively, you can pose an open-ended question for them to think about. Have them write about it (with a 'quick write') and then report their initial thinking to their group. Providing students time to think and write individually before sharing in the group is often helpful. Not all students want to start talking right away.

Another workable method is to set aside a portion of class time for students to discuss a concept or work on a problem, an investigation, or a group project. Some, or all, groups can report on their work to the class (either as a progress report or a final report). You can add perspective and background information as needed. In a large class, where it is cumbersome to use groups, you might have the students spend some time working in pairs—discussing a definition, sharing thoughts about a problem, comparing solutions or exploring a concept. Your Teaching Assistant can, with some encouragement from you, use small groups in discussion sections.

In order to ease the transition from lectures, provide an experience early on in the course demonstrating that a small group approach enhances learning in ways that lectures do not. For example, I often begin my class on problem solving with *Counting Squares*. Students are given a problem (FIGURE 1) and asked to work individually.

Counting Squares
(individual)

How many squares are there in the figure below? Be able to defend your answer. Work by yourself.

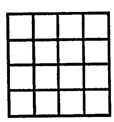


Figure 1

After about 10–15 minutes they are arranged in groups and given the problem in FIGURE 2.

Counting Squares
(small groups)

How many squares are there in the figure below? Work in your groups. Make sure that everyone is able to defend the answer.

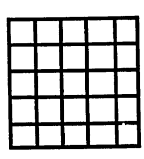


Figure 2

After the activity, I ask them to reflect on the process with the following instructions: Each person tells how they felt when doing the problem alone and as a group. Discuss the differences between individual learning and small group learning.

Another activity that shows students how small groups can enhance learning is Missing Corners. In this activity the students are asked to (individually) write a description of the pattern in FIGURE 3, construct with cubes (or tiles) the next two figures in the pattern, predict the number of cubes in the *n*th figure and write a justification for their prediction based on the figures. The students are amazed when they arrive at different ways of describing the pattern and justifying the predictions. (This can be followed by examining more complex, even 3-dimensional, patterns.)

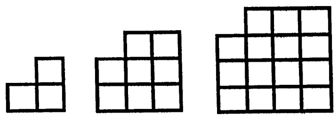


Figure 3

One obstacle when college students begin to work in groups is their lack of experience communicating about mathematics. It is important therefore that early group activities develop communication skills rather than stress solutions or proof. A colleague of mine, Bill Jacob, addresses this issue in a geometry class by having one student draw a geometric figure, a second write instructions on how to draw the figure for a third student, who then draws the figure without having seen the original figure. The figures are compared and the results discussed. Then the roles are rotated. He also has the students write reports on experiments (for example, projective geometry experiments with mirrors).

There are not many examples of college level curriculum written specifically for small group instruction. Two older texts [**5**, **12**] attempt to present traditional course content for a small group approach. There is more available for the pre-college level and these sources may provide ideas for what can be done at the college level. The Interactive Mathematics Project[1] and the California Math A materials[2] are good examples of non-traditional approaches at the secondary level. Bishop [**1**] is a good resource for thinking about how to restructure curriculum for group projects and discussion. I used *Thinking Mathematically* [**7**] successfully in a problem solving course for potential secondary teachers. A good source for reading about what other people have done is [**4**]. Be aware, however, that some of the authors in this book have a very traditional view of mathematics and there is considerable disagreement about classroom practices as well.

It may be necessary to change your ideas of "covering" curriculum. It will help to reflect on the questions: what does it mean to teach? what does it mean to learn? College faculty need to think about and discuss the relative value of exposing students to mathematical knowledge or having them actually do mathe-

[1]This project is developing a three year problem-based mathematics high school mathematics course. Contact Interactive Mathematics Project-EQUALS, University of California, Berkeley, CA 94720.

[2]This material was developed by California secondary teachers to meet the guidelines of the 1985 California Framework. It is being rewritten by Larry Hatfield for publication by Glencoe Publishing Company in June, 1993.

matics. For example, a class for potential secondary teachers explored symmetry by examining some strip patterns from Native American (San Ildefonso Pueblo) pottery. I then asked them to create their own strip patterns with pattern blocks (colored squares, triangles, trapezoids, parallelograms, and hexagons). I then asked the students to classify the strip patterns. With very little help from me most groups (in three to four hours of class time) discovered the seven different classes and were able to justify (although not rigorously) that these were all of them. I could have lectured about it in an hour or two, but I think that the level of understanding would have been shallower. There are no easy answers to questions about breadth versus depth—perhaps no answers at all—but it is beneficial to reflect on and discuss the questions.

STUDENTS. Students will probably be skeptical about participating in a small group at first. You need to explain to them why you are deviating from the traditional lecture method—and remind them periodically of your reasons and "philosophy of education". Some students may continue to struggle with the different approach:

> *Once again as in Math 101A I have mixed feelings arising out of working in groups. One thing, working in small groups tends to make* me *more visible to others. That means my strong points, in between points, and weak points are right there for everyone to see. It is very hard for me to expose my weaknesses to others, i.e., my mistakes. Working in small groups tends to make me confront a feeling of stupidity. It is hard to overcome the urge to compare myself to others and to try to come up with the correct answer. I tend to underplay 'correct' contributions (i.e., a good idea) and overplay any errors I make, so it tends to be a struggle for me.*

Others will make the transition more readily:

> *To be honest, when this class first began I did not enjoy it very much. It is hard for me to pin down why. In part it had a bit to do with the groups. It was not the fact that I did not know my group yet. I knew that we all would get to know one another. It was more because the people in my group seemed to be so much brighter than me. It did not seem as if I would ever have anything worth while to contribute .... After a few weeks of classes we all felt comfortable. We not only discussed math topics but also what we did over the weekend. How things were going etc. It was no longer a state of unfamiliarity or any anxiety over making a mistake or saying something foolish ... [If we had not been in a group] I do not think we would have become friends.*

Many come to understand and value the benefits of small group instruction:

> *Working in small groups is very different than lecturing only. There is no strict relationship where one person knows all the answers (teacher) and the other asks the questions (student). Working in a group is a more equal relationship where hopefully everyone is answering and asking questions. I like working in a small group, because it forces you to think rather than just copy whatever the teacher writes.*

> *To be honest, in the past the only method that I knew to learn mathematics was to memorize so, therefore, if I memorized the material well I felt pretty good as a learner, but now, however, I realize that I have been somewhat cheated on what and how I learned mathematics. It just seems like I should have a better understanding of what I have learned in the past.*

It is important to pay attention to the quality of the group process. Every three to four weeks I have students assess their group's functioning. I ask them to answer two questions in their weekly journal: What are you doing to contribute to the group's functioning well? What can you do to improve? Then I visit each group and sit down with them and ask each person to talk about their answers. This method provides them time to think about the questions free from pressure, but

ensures that the group is communicating about group processes. It also indicates clearly that I value group process, since I devote my time to assessing it.

Take time to interact with students. They will be uneasy about working in groups and will need time to talk about it. The relationship with the instructor is crucial in making the small group approach work. One student addressed the issue in his journal:

I believe that a very useful addition to this course would be to require, perhaps during the second or third weeks, each student to make an appointment during office hours. I believe a one on one discussion on 'what do you want to get out of this course?' to 'what do you want to get out of teaching?' would enhance the entire course. I believe that it would make the students even more aware of what they can get out of the course, as well as, being aware of the usefulness of being available to students for one-on-one talks. Offering offices hours does a lot. However, requiring us to take advantage of office hours would be excellent.

Be aware of the effect of grading on small groups. The first day (of a course in problem solving for prospective secondary teachers) I told the students how I would grade (see FIGURE 4) and in particular that I did not value memorization but would assess progress in their mathematical reasoning and their ability to communicate (verbally and in writing) about mathematics. I told them that I wanted to try (for the first time) using student portfolios to assess their work.

Attendance	10%;
Contribution to group and class (including an assessment of a portfolio of their work)	20%
Five problem sets	30%
Journal	20%
Final exam (oral)	20%

Figure 4

They were a little uneasy about this, so in the third week of the semester I spoke more about my philosophy, grades, and what portfolios were. I asked them to suggest what kind of evidence would show growth in mathematical thinking. We made a list and I indicated that they should include this type of evidence as part of their portfolio. Because I had devised what I thought would be a very acceptable grading method, and spent some time in class discussing it, I was surprised to read what one student wrote in her journal:

The assessment lecture bothered me. Up to that day working in the groups and learning was fun. I had been thoroughly enjoying the class but when the portfolio came up and I realized that something was going to be 'graded' my perspective of the class began to change. All of a sudden I had to pay attention to what I was writing down. 'Is it neat enough?' Am I writing enough?' 'Have I misplaced something that I should have kept?' These questions and slight panic began to be aroused in me. That day our group discussion was much more jumpy and less relaxed. For the first time our ideas came across in a competitive way. I cannot really explain why we became more interested in getting our ideas on paper than playing with the problem. With the knowledge that our progress was going to be measured, our performance became more forced and less enjoyable.

I have not solved the problem raised by this student. Certainly anxiety about grades is not unique to the small group approach. I have long believed that any "outside" (by someone other than the learner) evaluation of learning interferes with the learning process—with the possible exception of assessment conducted as an integral part of the learning process with the goal of assisting the learner. Furthermore I consistently find that my dual responsibilities of facilitating learning

and evaluating it, are inconsistent. Ideally a learner would be willing to reveal his/her ignorance to a teacher. In reality, he/she may be reluctant to do so to an evaluator. Although the small group approach reduces the interference of grades with learning (for example, anxiety is reduced by talking about grades with friends, students are graded on more than just test results) it does not eliminate it. I am not comfortable with grading and I admit my dilemma to my students. After reading the above student's journal, I read the passage (anonymously) to the class and we discussed grades, competition and learning. It seemed to help.

While on the subject of assessment, it is worth pointing out the obvious. Often students memorize to get by on tests. Success in this system does not necessarily mean that students have learned (understood and are able to use) the mathematics. We often do not notice this when using the lecture method because we only see test results. When you observe students working in groups, however, you will see more clearly what students do and do not understand. It can be disconcerting. In a class on classical number systems, for example, I asked students to use a concrete model to justify the familiar algorithm for adding fractions. They had tremendous difficulty coming up with an explanation.

A final point in regard to your students: Do not be too hard on them. There is an old saying "Don't blame the messenger who brings bad news." In a sense, undergraduates who cannot think or communicate well about mathematics are the message that something is drastically wrong with our education system. Small group instruction is not a panacea. It will not immediately remedy the deficiencies of previous miseducation. But it is a start.

INSTITUTIONAL AND PERSONAL SUPPORT. It will not be easy to give up the lecture method. Both institutional and personal support will be helpful in making the change. The Action Plan of *Moving Beyond Myths* makes many institutional recommendations. Draw these to the attention of relevant officials and organize on your campus for implementing the suggested reforms.

At present there is little opportunity for college faculty to participate in professional development focused on teaching. The educational community regards professional development in both content and methodology as a necessary part of *pre-college* teachers' professional growth. For college instructors, however, professional development focuses on learning more mathematics or on suggested revisions in content, not learning about new pedagogical approaches or research in mathematics education.

Until there is adequate opportunity to participate in professional development activities focused on teaching, individuals will have to strike out on their own. It may be possible to arrange your own professional development by watching someone who is using small groups or participating in a small group experience taught by someone else. In the long run, however, the attitudes and practices within the profession concerning professional development will need to change if large numbers of college faculty are to obtain the support necessary to implement the goals of the reform movement.

Even with institutional support for change you will need to get personal support if you intend to change your teaching. Find people with whom you can discuss mathematics teaching—your ideas, your successes and failures. (Accept that there will be failures.) In addition, find someone who is able to listen to you non-critically. It will be helpful to reflect on what you are doing and deal with your feelings about your efforts without fear of criticism. I did not have that 20 years ago and that is one reason why I abandoned my experimentation for three years. When you

are feeling tense or worried about whether you are doing the right thing you will tend to revert to the 'tried and true.' If you have someone to talk to about your feelings it is more likely that you will be able to think through the issues, and pursue your goals. See [**13**, **14**] for further information about the relationship between feelings, listening and educational change.

CONCLUSION. Teaching using small groups is very different from lecturing. You will need time to develop your abilities. Be prepared for ambivalence and doubts. I encourage you to persist. Virtually every teacher (elementary or secondary) takes mathematics courses in a college or university. How you teach mathematics to undergraduates affects mathematics education throughout the entire system. You can play a crucial role in modeling for future teachers how to teach so that students are actively engaged in doing mathematics. If you are satisfied with large numbers of students not understanding or liking mathematics, with an attrition rate for mathematics students of approximately 50% each year after 9th grade [**2**], then continue with the lecture method. But if you want to provide opportunities for larger numbers of students to gain deeper understandings and to improve their ability to communicate about mathematics, then explore small group approaches and other alternatives to the lecture method. Perhaps you will be rewarded by having a future secondary teacher write: *I want to implement in my classroom what we did in this class. The most important thing that I have learned is that math can be fun.*

REFERENCES

1. Bishop, A. J., "Mathematical Enculturation: A Cultural Perspective on Mathematics Education." 1988 Kluwer. Dordrecht.
2. Committee on the Mathematical Sciences in the Year 2000. "A Challenge of Numbers." 1990 National Academy Press. Washington, D.C.
3. Davidson, N., The Small Group Discovery Method as Applied in Calculus Instruction. *American Mathematical Monthly*. August–September: 789–91, 1971.
4. Davidson, N., *Cooperative Learning in Mathematics, A Handbook for Teachers*. 1989, Addison Wesley, Menlo Park.
5. Davidson, N. and F. Gulick, "Abstract Algebra: An Abstract Learning Approach." 1976 Houghton Mifflin. Boston.
6. MAA Committee on the Mathematics Education of Teachers. "*A Call for Change: Recommendations For The Mathematical Preparation Of Teachers Of Mathematics*." Leitzel ed. 1991 Mathematical Association of America. Washington, D.C.
7. Mason, J., L. Burton and K. Stacey, "Thinking Mathematically." 1985 Addison Wesley. Reading.
8. National Council of Teachers of Mathematics. "Professional Standards for Teaching Mathematics." 1991 NCTM. Reston.
9. National Research Council. "Everybody Counts: A Report to the Nation About the Future of Mathematics Education." 1989 National Academy Press. Washington, D.C.
10. National Research Council. "Moving Beyond Myths: Revitalizing Undergraduate Mathematics." 1991 National Academy Press. Washington, D.C.
11. Weissglass, J., Small Groups: An Alternative to the Lecture Method. *Two Year College Mathematics Journal*. (Now the *College Mathematics Journal*) 7:15–20, 1976.
12. _____, "Exploring Elementary Mathematics: A Small Group Approach for Teaching," 1979 Kendall-Hunt (originally published by W. H. Freeman.)
13. _____, Constructivist Listening for Empowerment and Change. *The Educational Forum*. 54(4):351–370, 1990.
14. _____, Teachers Have Feelings: What Can We do About It? *Journal of Staff Development*. (12(1)):28–33, 1991.

Mathematics Department
University of California
Santa Barbara, CA 93106

A Fast Pick-Type Approximation for Areas of H-Polygons

Ding Ren, Krzysztof Kołodziejczyk, Grattan Murphy, and John Reay

1. INTRODUCTION AND DEFINITIONS. Pick's formula $b/2 + i - 1$ gives the area of a simple polygon in R^2 whose corners lie in the integer lattice, and which has b lattice points on its boundary and i lattice points in its interior. It has been the object of many studies since its proof by Pick [6] in 1900. Throughout this paper we assume P is an *H-polygon*, i.e., a simple polygon whose corners lie in the set H of vertices of a monohedral tiling of R^2 by regular hexagons of unit area. See FIGURE 1 for examples. The vertices of this hexagonal tiling have density 2

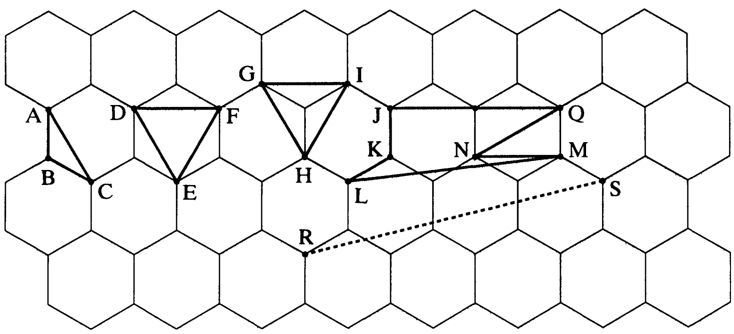


Figure 1. Mensurable H-polygons.

(that is, each hexagon may be associated with 2 vertices), in contrast to the points of the integer lattice used in Pick's theorem, which have density one. Therefore it is reasonable to define *Pick's approximation* for the area $\mu(P)$ of an H-polygon P by

$$F(P) = (b/2 + i - 1)/2. \tag{1}$$

For example, in FIGURE 1 if P is the triangle ABC or triangle DEF then $b = 3$, and $i = 0$, so Pick's approximation is $F(P) = 1/4$, while the true areas are $\mu(ABC) = 1/6$ and $\mu(DEF) = 1/2$. Also triangle GHI has area $\mu(GHI) = 1/2$ and approximation $F(P) = (3/2 + 1 - 1)/2 = 3/4$. In the next section we find bounds on the size of the error of this Pick-type approximation for the area; this will show that $F(P)$ is, in some sense, a very good approximation.

The exact area of many H-polygons, like those in FIGURE 1, may be found by computing one additional parameter, the boundary characteristic. Every vertex $X \in H$ of the hexagonal tiling that is also on the boundary ∂P of P is the endpoint

of 3 edges of the hexagonal tiling. Define the *boundary characteristic* $c(X, P)$ *of* P *at* X to be the number of those 3 edges that extend locally into the exterior of P from X, minus the number that extend locally into the interior of P from X. Then the *boundary characteristic* of P is defined as $c = c(P) = \Sigma_{X \in H \cap \partial P} c(X, P)$. For example, if P is the irregular hexagon $JKLMNQ$ in FIGURE 1, then $b = 7$, $i = 0$, and $c = 2 - 1 + 2 + 3 - 3 + 3 + 1 = 7$. If points of H occur frequently along the boundary ∂P of P (specifically, if the neighboring H-points on ∂P are closer than the distance from R to S in FIGURE 1), then it is shown in [**2**] that the area $\mu(P)$ of P is given exactly by

$$A(P) = b/4 + i/2 + c/12 - 1. \tag{2}$$

(This is easily checked for the examples in FIGURE 1.) An H-polygon is called *mensurable* if $\mu(P) = A(P)$. The mensurable H-triangles have been characterized in [**5**]. Using the Pick approximation $F(P)$ for the area of P is faster than computing areas with (2) since it saves the computation of the boundary characteristic. In the next section we first get sharp inequalities between the parameters b and c for H-polygons, and then use them to justify the use of the fast Pick's approximation. Scott [**7**] and Coleman [**1**] have considered similar inequalities between b and i for convex polygons with corners in the integer lattice. See [**4**] and [**8**] for related results and further bibliography on Pick's Theorem.

2. BOUNDARY CHARACTERISTIC BOUNDS AND PICK'S APPROXIMATION. Let P denote any simple H-polygon with $b = |H \cap \partial P|$ and boundary characteristic c. Triangles GHI and DEF of FIGURE 1, (and other examples with any $b \geq 3$) show that the inequalities in the following theorem are sharp.

Theorem 1. *For any simple H-polygon*, $-b \leq c - 6 \leq b$.

Theorem 1 may be used to provide a bound on the size of the error which occurs in using Pick's formula $F(P)$ to approximate the area $\mu(P)$ of mensurable H-polygons.

Theorem 2. *If P is a mensurable H-polygon then*

$$|F(P) - \mu(P)| \leq b/12.$$

Proof: If P is a mensurable H-polygon then $A(P)$ in formula (2) gives the exact area $\mu(P)$ of P. Use the inequalities $c \leq b + 6$ and $c \geq -b + 6$ from Theorem 1 to replace c in the formula (2), and simplify. The result is immediate. ∎

The triangles in FIGURE 1 show that the bound in Theorem 2 cannot be improved in general.

Proof of Theorem 1: We will choose a point in the relative interior of a side of P and traverse the boundary ∂P once in a counterclockwise direction, keeping track of changes in two parameters, the boundary characteristic and the deflection number, which will change only at points of $H \cap \partial P$. The *deflection number* as used in this proof will be defined in Table 1 for each $X \in H \cap \partial P$ in such a way

that it is always an integer multiple of $1/6$. The sum of the deflection numbers over all such X will agree with the *rotation number of P* as defined in [**3**] and [**4**], and will always be 1, which represents the fact that the direction of travel makes one complete rotation (of 2π) as we traverse once around ∂P in a counterclockwise direction. We may assume that the tilting at a typical vertex $X \in H \cap \partial P$ is oriented as shown in FIGURE 2, so that the 3 edges of the tiling which meet at X,

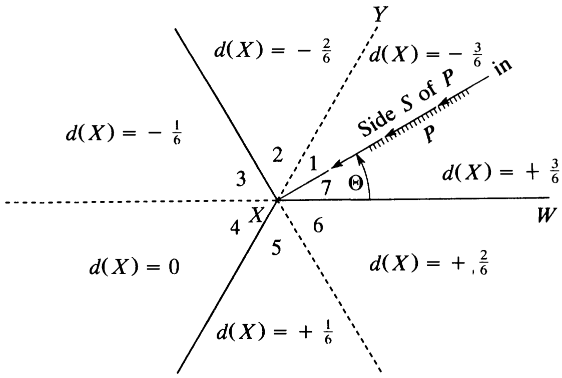


Figure 2. Sectors determined by a typical $X \in H \cap \partial P$.

together with their reflections in X, form 6 sectors about X, each of size $\pi/3$. Then the side S of P being traversed either approaches vertex X along the segment WX which is parallel to a tiling edge, or through the interior of sector WXY (as shown in FIGURE 2) thereby dividing sector WXY into 2 smaller sectors. In either case, let Θ be the angle between WX and side S, with $0 \leq \theta < \pi/3$. The sectors (numbered 1 through 7 in FIGURE 2) and the deflection number $d(X)$ for each sector are defined in Table 1.

TABLE 1. Deflection number when the boundary traverse leaves X in sector i. (Sector 7 does not exist if $\Theta = 0$ and side S contains WX.)

Sector Number	Angle ϕ from XW to leaving side	Deflection No. $d(X)$
1	$\Theta \leq \phi < \pi/3$	$-3/6$
2	$\pi/3 \leq \phi < 2\pi/3$	$-2/6$
3	$2\pi/3 \leq \phi < \pi$	$-1/6$
4	$\pi \leq \phi < 4\pi/3$	0
5	$4\pi/3 \leq \phi < 5\pi/3$	$1/6$
6	$5\pi/6 \leq \phi < 2\pi$	$2/6$
7	$0 \leq \phi < \Theta$	$3/6$

We distinguish three types of vertices $X \in H \cap \partial P$ depending on how the boundary passes through X on our traverse:

Type 1. The boundary traverse approaches X along side S with $\Theta > 0$ (as shown in FIGURE 2) and leaves X through the interior of some sector, or else, the traverse approaches X along WX (so $\Theta = 0$ and Sector 7 does not exist) and leaves X on a side parallel to an edge.

TABLE 2. Bounds for the boundary characteristics.

Sector Number	Type 1 c_M	Type 1 c_m	Type 2 c_M	Type 2 c_m	Type 3 c_M	Type 3 c_m
1	-3	-3	(no such vertices)		-2	-3
2	-1	-3	-2	-3	-1	-2
3	-1	-1	-1	-2	0	-1
4	1	-1	0	-1	1	0
5	1	1	1	0	2	1
6	3	1	2	1	3	2
7	3	3	3	2	(no such vertices)	

Type 2. Angle $\Theta > 0$ and the traverse leaves X on a side which is parallel to an edge.

Type 3. The traverse approaches X along WX (so $\Theta = 0$) and leaves through the interior of some sector.

Table 2 shows the maximum $c_M(X, P)$ and minimum $c_m(X, P)$ possible values of $c(X, P)$, when vertex X is of each of the above 3 types. It will follow from the definition of the deflection number that

$$\sum_{X \in H \cap \partial P} d(X) = 1 \tag{3}$$

First, suppose that for each vertex X of P, our traverse of P always both approaches X and leaves X in the exact center of one of the 6 sectors of size $\pi/3$ shown in FIGURE 2. For this special case of P, the deflection number at each X agrees with the rotation number, takes a value from the discrete set $\{k/6 | k = -2, -1, \ldots, +2\}$, and sums (over all $X \in H \cap \partial P$) to 1 full rotation. Hence (3) holds. To show (3) for a general H-polygon P, note that for each edge $\langle X, V \rangle$ of P the angle between $\langle X, V \rangle$ and the center of the sector it enters at X is exactly the negative of the angle between $\langle X, V \rangle$ and the center of the sector which it leaves at V. Thus the sum of the angle deflections is the sum of the deflection numbers and (3) holds for general P.

It is also clear that

$$c_L := \sum_{X \in H \cap \partial P} c_m(X, P) \le c \le \sum_{X \in H \cap \partial P} c_M(X, P) =: c_U \tag{4}$$

by the definition of the boundary characteristic. Define t_{ij} to be the cardinality of the set $\{X \in H \cap \partial P | \partial P$ leaves X in sector i, and X is of type $j\}$ for $i = 1, 2, \ldots, 7$. Then $b = \sum_{i \in \{1,2,\ldots,7\}} \sum_{j \in \{1,2,3\}} t_{ij}$ and (3) may be rewritten (denoting $\sum_j t_{ij}$ by t_i) as

$$6 = -3t_1 - 2t_2 - t_3 + t_5 + 2t_6 + 3t_7 \tag{3'}$$

and the right side of (4) becomes

$$\begin{aligned} c \le -3t_{11} - t_{21} - t_{31} + t_{41} + t_{51} + 3t_{61} + 3t_{71} \\ - 2t_{22} - t_{32} + t_{52} + 2t_{62} + 3t_{72} \\ -2t_{13} - t_{23} + t_{43} + 2t_{53} + 3t_{63} = c_U. \end{aligned} \tag{4'}$$

Using the above expressions for b, 6, and c_U in terms of the t_{ij}'s, it follows that

$$6 + b = c_U + [t_{11} + t_{31} + t_{51} + t_{71}] + t_{22} + t_{32} + t_{42} + t_{52} + t_{62} + t_{72} \geq c_U \geq c.$$

Using the left inequality of (4) in a similar way it follows that

$$6 - b = c_L - \left([t_{11} + t_{31} + t_{51} + t_{71}] + \sum_i t_{i3}\right) \leq c_L \leq c.$$

This gives the desired inequalities. ■

REFERENCES

1. D. B. Coleman, Stretch: a geoboard game, *Math. Mag.*, 51 (1978) 49–54.
2. R. Ding, K. Kołodziejczyk and J. Reay, A new pick-type theorem on the hexagonal lattice, *Discrete Math.* 68 (1988) 171–177.
3. B. Grünbaum and G. Shephard, Rotation and winding numbers for planar polygons and curves, *Trans. Amer. Math. Soc.* 322 (1990) 169–188.
4. B. Grünbaum and G. Shephard, Pick's theorem, *Amer. Math. Monthly* 100 (1993) 150–161.
5. K. Kołodziejczyk and J. Reay, Primitive and mensurable hex-triangles, *Geometriae Dedicata* 15 (1992) 233–241.
6. G. Pick, Geometrisches zur Zahlenlehre, *Sitzungsber. Lotos. Prag.*, 19 (1900) 311–319.
7. P. R. Scott, On convex lattice polygons, *Bull. Austral. Math. Soc.*, 15 (1976) 395–399.
8. P. R. Scott, The fascination of the elementary, *Amer. Math. Monthly*, 94 (1987) 759–768.

Hebei Teachers University
Shijiazhuang, People's Republic of China

Instytut Matematyki
Politechniki Wrocławskiej
Wrocław, Poland

Mathematics Department
University of Maine
Orono, ME 04469

Mathematics Department
Western Washington University
Bellingham, WA 98225

Logarithmetica Britannica. Being a Standard Table of Logarithms to Twenty Decimal Places. By Alexander John Thompson. Part V, Numbers 50000 to 60000 Issued by the Biometric Laboratory, University of London, to Commemorate the Tercentenary of Henry Briggs' Publication of the *Arithmetica Logarithmica*, 1624. Subscription Issue. Cambridge, The University Press, 1931.

This is the fifth part (the fourth not yet published) of this tremendous undertaking. It consists of twenty-place logarithms of numbers of five digits, accompanied by values of second and fourth differences. The project speaks for itself; it is sufficient to say that the result is all that is to be expected of any product of the Cambridge Press.

—*American Mathematical Monthly*
38, (1931) p. 407

NOTES

Edited by: **John Duncan**

A Simple Example on Non-Sequentialness in Topological Spaces

Heinz König

There are well-known examples of countable Hausdorff topological spaces which are not discrete but show certain typical features of discreteness: all compact subsets are finite, and therefore all convergent sequences are ultimately constant. These spaces are of interest in functional analysis and measure theory. The examples known to the present author are due to Arens [**1**] and Varadarajan [**6**]. This note wants to add a different example which is strikingly simple. It arose in [**5**] in connection with the double limit relation.

THE NEW EXAMPLE. We fix a sequence (t_n) of real numbers $t_n > 0$ such that $t_n \to 0$ for $n \to \infty$ and $\sum_{n=1}^{\infty} t_n = \infty$ (for example $t_n = 1/n$). We call a subset $S \subset \mathbb{N}$ *small* iff $\sum_{n \in S} t_n < \infty$, which is to include $S = \varnothing$. Thus all finite subsets of $\mathbb{N}$ are small, but there are also infinite small subsets: in fact, each infinite subset of $\mathbb{N}$ contains a small infinite subset. By means of the small subsets of $\mathbb{N}$ one then forms a topology on $X := \mathbb{N} \cup \{\infty\}$, with the open sets defined to be i) all subsets $A \subset \mathbb{N}$, and ii) those subsets $A \subset X$ with $\infty \in A$ whose complements $A' \subset \mathbb{N}$ are small. It is obvious that this is a Hausdorff topology on X which is not discrete, and it is a simple verification that all compact subsets of X are finite.

We turn to the two previous examples. Each time the above rôle of the small subsets of $\mathbb{N}$ will be assumed by some other set system σ on $\mathbb{N}$.

The example of Arens (see also Kelley [**4**] Problem 2.E and Engelking [**3**] Example 1.6.20). We fix a sequence (X_n) of pairwise disjoint infinite subsets $X_n \subset \mathbb{N}$ with union $\mathbb{N}$. Then we define σ to consist of the subsets $S \subset \mathbb{N}$ such that $S \cap X_n$ is finite for almost all n.

The example of Varadarajan (see also Berg-Christensen-Ressel [**2**] Exercise 2.1.30). We define σ to consist of the subsets $S \subset \mathbb{N}$ such that

$$\frac{1}{n}\operatorname{card}(S \cap \{1, \dots, n\}) \to 0 \quad \text{for } n \to \infty.$$

Thus each time we have a system σ of subsets of $\mathbb{N}$, intended to form the *small* subsets of $\mathbb{N}$, with the properties

1) σ contains all finite subsets of $\mathbb{N}$;
2) $S \in \sigma$ implies $T \in \sigma$ for all $T \subset S$;

3) σ is stable under finite unions;
4) $\mathbb{N}$ is not a member of σ;
5) each infinite $S \subset \mathbb{N}$ contains an infinite $T \in \sigma$.

In each of the two previous examples properties 1)–4) are obvious and 5) requires a little proof. In the new example all properties are obvious.

By means of a set system σ on $\mathbb{N}$ with the above properties 1)–5) one then forms a topology τ on $X := \mathbb{N} \cup \{\infty\}$, with the open sets defined to be i) all subsets $A \subset \mathbb{N}$, and ii) those subsets $A \subset X$ with $\infty \in A$ whose complements $A' \subset \mathbb{N}$ are members of σ. We collect the main consequences in the proposition below, the proof of which can be left to the reader as a sequence of simple exercises. We note that the last assertion is independent of condition 5) above.

Proposition. 1) *τ is a Hausdorff topology on X which is not discrete.* 2) *Each compact subset (and even each relatively countably compact subset) of X is finite. Therefore each convergent sequence in X is ultimately constant.* 3) *τ is completely normal: each nonvoid subset of X is normal in its relative topology.*

In particular the subset $\mathbb{N} \subset X$ has the cluster point ∞. Also the sequence (x_n) of the points $x_n = n$ has the cluster value ∞. But there is no sequence in $\mathbb{N}$ which converges to ∞.

Thus we have a common scheme for all the above examples. It is obvious that the new example is particularly simple.

There is also the notorious non-constructive example: By Zorn's lemma, each set system σ on $\mathbb{N}$ with properties 1)–4) (for example the system of all finite subsets) is contained in a maximal such set system (in order to work with the usual notions of filters and ultrafilters one has to pass to complements). We claim that each set system σ on $\mathbb{N}$ which is maximal with respect to properties 1)–4) also satisfies 5), and hence produces a topology τ on $X := \mathbb{N} \cup \{\infty\}$ as above. To see this note first that for each $T \subset \mathbb{N}$ one has either $T \in \sigma$ or $T' \in \sigma$. Now fix an infinite $S \subset \mathbb{N}$. We write $S = P \cup Q$ with disjoint infinite $P, Q \subset S$. In case $P, Q \notin \sigma$ then $P', Q' \in \sigma$ and hence $\mathbb{N} = (P \cap Q)' = P' \cup Q' \in \sigma$, which is not true. Thus we have a $P \in \sigma$ or $Q \in \sigma$. This proves 5).

The author wants to thank the referee and the Notes editor for good advice.

REFERENCES

1. R. Arens, Note on convergence in topology. *Math. Mag.* 23 (1950), 229–234.
2. J. Berg, J. P. R. Christensen and P. Ressel, *Harmonic Analysis on Semigroups*, Springer, 1984.
3. R. Engelking, *General Topology*, Heldermann, Berlin, 1989.
4. J. L. Kelley, *General Topology*, Van Nostrand 1955.
5. H. König and N. Kuhn, Angelic spaces and the double limit relation, *J. London Math. Soc.* (2) 35 (1987), 454–470.
6. V. S. Varadarajan, Measures on topological spaces, *AMS Transl.* (II) 48 (1965), 161–228.

Universität des Saarlandes
Fachbereich Mathematik
D-66041 Saarbrücken / Germany

The Secant Method and the Golden Mean

Melvin J. Maron and Robert J. Lopez

The secant method is a well-known method for finding roots α of the equation $f(x) = 0$. Starting with two initial approximations of α, say x_{-1} and x_0, the secant method generates

$$x_{k+1} = x_k - \frac{f(x_k)(x_k - x_{k-1})}{f(x_k) - f(x_{k-1})}, \qquad k = 0, 1, 2, \ldots \tag{1}$$

The rate at which the sequence $\{x_k\}$ converges to a root α depends on the multiplicity of α. Recall that α is a root of *multiplicity* m of the function f if $f(x)$ can be written as

$$f(x) = (x - \alpha)^m \phi(x), \quad \text{where } \phi \text{ is bounded at } \alpha \text{ and } \phi(\alpha) \neq 0. \tag{2}$$

It is well known (see [2]) that if α is simple root, that is, if $m = 1$, then there will be a nonzero asymptotic error constant C such that the errors

$$\varepsilon_k = \alpha - x_k$$

satisfy

$$\lim_{k \to \infty} \frac{|\varepsilon_k|}{|\varepsilon_{k-1}|^p} = C, \quad \text{where } p = \frac{\sqrt{5} + 1}{2} = 1.618 \cdots.$$

Thus, secant method iterates will converge superlinearly with order $p = \frac{1}{2}(\sqrt{5} + 1)$ to simple roots α. Ancient Greek mathematicians attached profound significance to the numbers

$$r = \frac{\sqrt{5} - 1}{2} = 0.618 \cdots \quad \text{and} \quad p = r + 1 = \frac{1}{r} = \frac{\sqrt{5} + 1}{2} = 1.618 \cdots. \tag{3}$$

They referred to r as the *golden mean* because the ratio $(1 - r) : r$ equals r. Observe that r and $-p$ are the roots of the quadratic equation

$$x^2 + x - 1 = 0. \tag{4}$$

The purpose of this paper is to prove the following result[1], which shows that the golden mean is also related to the way secant method approximants converge to double roots.

Theorem. *Suppose α is a root of f for which*

$$f(x) = (x - \alpha)^2 \phi(x), \quad \text{where } \lim_{x \to \alpha} \phi(x) \neq 0, \tag{5}$$

[1] Part (a) was obtained for $f(x) = x^2(x - 1)^2$ and $\alpha = 1$ in [1] (Example E-11, p. 278).

and let $\varepsilon_k = \alpha - x_k$, where x_k is the kth approximant generated by secant method (1).

(a) If the sequence $\{x_k\}$ converges to α and $\lim_{k\to\infty}(\varepsilon_k/\varepsilon_{k-1})$ exists, then

$$\lim_{k\to\infty} \frac{\varepsilon_k}{\varepsilon_{k-1}} = r, \quad \text{where } r = \frac{\sqrt{5}-1}{2} = 0.618\cdots.$$

(b) For x_{k-1}, $x_k \approx \alpha$ and $\rho_k = \varepsilon_k/\varepsilon_{k-1} \approx r$, the ratios ρ_k will satisfy

$$\rho_{k+1} - r \sim -r^2(\rho_k - r) + r\left[\frac{\phi(x_{k-1})}{\phi(x_k)} - 1\right] \tag{6}$$

It follows that $\{\rho_k\}$ will converge to r once x_{k-1} and x_k are sufficiently close to α and ρ_k is sufficiently close to r.

Proof: (a) Since $x_k - x_{k-1} = (x_k - \alpha) + (\alpha - x_{k-1}) = \varepsilon_{k-1} - \varepsilon_k$, we have from (1)

$$\varepsilon_{k+1} = \alpha - x_{k+1} = \varepsilon_k + \frac{f(x_k)(\varepsilon_{k-1} - \varepsilon_k)}{f(x_k) - f(x_{k-1})}. \tag{7}$$

In view of (5), we may assume x_{k-1} and x_k to be sufficiently close to α so that ε_k, $\phi(x_k)$, and $f(x_k) = \varepsilon_k^2\phi(x_k)$ are all nonzero. Under this assumption, we can rearrange (7) to get

$$\frac{\varepsilon_{k+1}/\varepsilon_k - 1}{1 - \varepsilon_{k-1}/\varepsilon_k} = \frac{1}{f(x_{k-1})/f(x_k) - 1}, \tag{8}$$

where $f(x_{k-1})/f(x_k) = \phi(x_{k-1})/\phi(x_k) \cdot (\varepsilon_{k-1}/\varepsilon_k)^2$. Upon introducing the ratios

$$\rho_k = \frac{\varepsilon_k}{\varepsilon_{k-1}} \quad \text{and} \quad \beta_k = \frac{\phi(x_{k-1})}{\phi(x_k)}, \quad \text{for } k = 1, 2, \ldots$$

in (8) and using the assumption $\lim_{x\to\alpha}\phi(x) \neq 0$, we get

$$\frac{\rho_{k+1} - 1}{\rho_k - 1} = \frac{\rho_k}{\beta_k - \rho_k^2}, \quad \text{where } \lim_{k\to\infty} \beta_k = 1. \tag{9}$$

So if $\lim_{k\to\infty}\rho_k$ exists, it must be a solution of the equation $(x-1)(x^2+x-1) = 0$, that is 1, r, or $-p$. Since $\lim_{k\to\infty}\rho_k$ cannot be zero, $\{x_k\}$ cannot converge superlinearly to α; however, linear convergence requires $|\lim_{k\to\infty}\rho_k| \leq 1$. But $\lim_{k\to\infty}\rho_k$ cannot be 1 because if it were, then

$$|\rho_{k+1} - 1| < |\rho_k - 1|, \quad \text{that is,} \left|\frac{\rho_{k+1} - 1}{\rho_k - 1}\right| < 1$$

would hold for infinitely many k's in (9), whereas $|\rho_k/(\beta_k - \rho_k^2)| > 1$ would hold for sufficiently large k. This leaves r as the only possible asymptotic error constant.

(b) To obtain (6), we first rewrite (9) as the finite difference equation

$$\rho_{k+1} = \frac{\rho_k - \beta_k}{\rho_k^2 - \beta_k}, \qquad k = 0, 1, 2, \ldots. \tag{10}$$

and then subtract r to get

$$\begin{aligned}
\rho_{k+1} - r &= \frac{\rho_k - \beta_k}{\rho_k^2 - \beta_k} - r \\
&= \frac{\rho_k - \rho_k^2 r - \beta_k(1-r)}{\rho_k^2 - \beta_k} \\
&= \frac{\rho_k^2 r - \rho_k + \beta_k r^2}{\beta_k - \rho_k^2}. \qquad [1 - r = r^2]
\end{aligned}$$

Writing ρ_k as $(\rho_k - r) + r$ and collecting numerator terms gives

$$\begin{aligned}
\rho_{k+1} - r &= \frac{(\rho_k - r)^2 r + (\rho_k - r)(2r^2 - 1) + (r^3 - r + \beta_k r^2)}{\beta_k - \rho_k^2} \\
&= \frac{r}{\beta_k - \rho_k^2}\{(\rho_k - r)(\rho_k - 1) + r(\beta_k - 1)\} \qquad [r^2 - 1 = -r] \\
&= \frac{r(\rho_k - 1)}{\beta_k - \rho_k^2}(\rho_k - r) + \frac{r^2}{\beta_k - \rho_k^2}(\beta_k - 1). \qquad (11)
\end{aligned}$$

Observe that if $\beta \to 1$ and $\rho \to r$, then

$$\frac{r(\rho - 1)}{\beta - \rho^2} \to \frac{r(r-1)}{1 - r^2} = \frac{-r}{1+r} = -r^2$$

[see (3)] and, similarly, $r^2/(\beta - \rho^2) \to r^2/(1 - r^2) = r$. It thus follows from (11) that

$$\rho_{k+1} - r = (-r^2 + \mu_1)(\rho_k - r) + (r + \mu_2)(\beta_k - 1)$$

where $|\mu_1|$ and $|\mu_2|$ can be made arbitrarily small by keeping $|x_k - \alpha|$ and $|\rho_k - r|$ sufficiently small. This implies (6) and completes the proof of the theorem. □

Traub [**1**, p. 278] states that secant method iterates will converge linearly to roots of any multiplicity $m > 1$. However, the authors are aware of no proof of this plausible assertion in [**1**] or elsewhere.

REFERENCES

1. J. F. Traub, *Iterative Methods for the Solution of Equations*, Prentice Hall, Englewood Cliffs New Jersey, 1964.
2. M. Vianello and R. Zanovello, On the Superlinear Convergence of the Secant Method, *American Mathematical Monthly*, 99 8 (1992) 758–761.

Engineering Mathematics and Computer Science Department
University of Louisville
Louisville, KY 40292
mjmaro01@ulkyvx.louisville. edu

Mathematics Department
5500 Wabash Avenue
Rose-Hulman Institute of Technology
Terre Haute, IN 47803
lopez@rose-hulman.edu

R_n Contains a Division Ring iff R Does

Ayman Badawi

INTRODUCTION. Let R be a ring with 1, and let R_n denote the complete matrix ring of all $n \times n$ matrices over R under the usual matrix addition and multiplication. Recall $A, B \in R_n$ are similar iff there exists $P \in R_n$ such that $A = PBP^{-1}$. If $A \in R_n$ is similar over R to a diagonal matrix, then A is called [1] diagonable over R. For $B \in R_n$, b_{ij} denotes the entry of B in the ith row and jth column.

In this note, we give an alternative proof of [1, Theorem 1] which is quite shorter than that in [1]. We would like to point out that our proof begins exactly like the original.

Theorem ([1, Theorem 1]). *Let R be a ring with* 1 *for which each idempotent matrix in* R_n *is diagonable over R. Then R contains a division ring if and only if* R_n *contains a division ring.*

Proof: If R contains a division ring, then clearly R_n contains a division ring. Assume R_n contains a division ring K. The division ring K has an identity—call it J—and by the hypothesis $PJP^{-1} = I$ a diagonal matrix for some invertible matrix $P \in R_n$. Since the conjugation of R_n by P induces a ring automorphism of R_n, $M = PKP^{-1}$ is a division ring of R_n and has I as the identity. Hence I is a nonzero idempotent of R_n. Let $S = \{A \in M\colon A \text{ is diagonal}\}$. Since $I \in S$, S is not empty. We leave it to the reader to verify that S is a division subring of M. Since $I \neq 0$, there exists $1 \leq j \leq n$ such that i_{jj} is a nonzero idempotent of R. Let $D = \{a_{jj}\colon A \in S\}$. Then D is a division ring of R with i_{jj} as the identity.

We end this note with some examples that satisfy the hypothesis of the Theorem and with one example where the hypothesis fails. Let R be a commutative ring with 1. Then R is called *ID* (basal) as in [7] ([2]) iff for every $n \geq 1$ the idempotents of R_n are diagonizable. Foster [2] has shown that if R is a principal ideal domain, then R is *ID*. Seshadri [6] has shown that if R is a principal ideal domain, then $R[x]$ is *ID*. In particular if F is a field, then $F[x, y]$ is *ID*. Steger [7] has shown that if R is an elementary division ring (i.e., for every $n \geq 1$ and $A \in R_n$ there exist invertible matrices P, Q in R_n such that PAQ is diagcnal) then R is *ID*. Also; Steger has shown that if R is π-regular ring (i.e., for every x in R there exists $n \geq 1$ and y in R (n and y depending on x) such that $x^n y x^n = x^n$) then R is *ID*. In particular for every $m \geq 1$ Z_m (i.e., Z/mZ) is *ID* (Foster has shown independently that Z_m is *ID*).

Finally, Theorem 3 in [7] states that if R is *ID*, then every invertible ideal of R is principal. Thus if R is a Dedekind domain which is not principal, then R is not *ID*. In particular, let $R = Z[\sqrt{-5}]$ (Z is the set of all integers). Then R is a Dedekind domain, see [4, EX. 37, P. 70]. But R is not a unique factorization domain, for example 21 does not have unique factorization in R. Thus R is not principal and therefore it is not *ID*.

REFERENCES

1. Jacob T. B. Beard, Jr. and Robert McConnel, Matrix fields over the integers modulo m, *Linear Algebra and Its Applications* 14, (1976), 95–105.
2. A. L. Foster, Maximal idempotent sets in a ring with unit, *Duke Math. J.* 13 (1946) 247–258.
3. L. Gilman and M. Henriksen, Some remarks about elementary divisor rings, *Tran. Amer. Math. Soc.* 82 (1956), 362–365.
4. Harry C. Hutchins, *Examples of Commutative Rings*, Harry C. Hutchings, 1981.
5. I. Kaplansky, Elementary divisors and modules, *Trans. Amer. Math. Soc.* 66 (1949), 464–491.
6. C. S. Seshadri, Triviality of vector bundles over affine space K_2, *Proc. Nat. Acad. of Sci. USA* 44 (1958), 456–458.
7. A Steger, Diagonability of idempotent matrices, *Pac. J. Math.* 19 (1966), 535–542.

Dedicated to Prof. Nick Vaughan on his retirement.

Department. of Mathematics
University of North Texas
Denton, TX. 76203

A Further Simplification of Dixon's Proof of Cauchy's Integral Theorem

Peter A. Loeb

The modification in [1] of Dixon's proof of the Cauchy Integral Theorem and Formula is based on the proposition stated below. In this note we give a proof of that proposition which is more suitable for undergraduate students. In what follows, G will be an open set in the complex plane $\mathbf{C}$, and γ will be a closed rectifiable curve. We write $f \in H(G)$ if f is holomorphic, i.e. analytic, in G, and we use the notation $D(z, r)$ for the disk $\{w \in \mathbf{C}\colon |w - z| < r\}$. The trace of γ in $\mathbf{C}$ is denoted by $\{\gamma\}$; we say the curve γ is in G when $\{\gamma\} \subset G$.

Proposition. *If γ is a curve in G, then for any $z \in \{\gamma\}$ there is a closed curve σ in G with $z \notin \{\sigma\}$ such that $\int_\gamma f = \int_\sigma f$ for all $f \in H(G)$.*

Proof: We assume that there is a point $\zeta \neq z$ with $\zeta \in \{\gamma\}$; otherwise the result is trivial. Pick $r > 0$ so that $D(z, r) \subset G$ and $\zeta \notin D(z, r)$. We will assume that γ is given by $\gamma(t)$ for $t \in [0, 1]$ and $\gamma(0) = \gamma(1) = \zeta$. By the uniform continuity of the mapping γ, there is a natural number n such that if $s, t \in [0, 1]$ and $|t - s| < 1/n$, then $|\gamma(t) - \gamma(s)| < r$. Partition the interval $[0, 1]$ using the points $0 < 1/n < \cdots < (n-1)/n < 1$. Let $0 = x_0 < x_1 < x_2 < \cdots < x_m = 1$ be the set of partition points k/n such that $\gamma(k/n) \neq z$. If between adjacent points x_i and x_{i+1} there is a point of the form k/n or any other point t_0 with $\gamma(t_0) = z$, then the path $\gamma(t)$, $x_i \leqslant t \leqslant x_{i+1}$, is in the disk $D(z, r)$. In this case, we may replace the

map γ on the interval $[x_i, x_{i+1}]$ with a path that goes from $\gamma(x_i)$ to $\gamma(x_{i+1})$ in the set $D(z, r) - \{z\}$. By Cauchy's integral theorem, applied to the disk $D(z, r)$, this replacement does not change the value of the integral for any $f \in H(G)$. With these replacements, the new path σ avoids z. □

REFERENCE

1. P. A. Loeb, A note on Dixon's proof of Cauchy's Integral Theorem, *American Mathematical Monthly* 98 (1991) 242–244.

Department of Mathematics
University of Illinois
1409 West Green St.
Urbana, Ill. 61801
LOEB@MATH.UIUC.EDU

Who Was the Author?

On an extension of Sir John Wilson's theorem to all numbers whatever, *Philosophical Magazine*, 1839.

Note on elimination, *Philosophical Magazine*, 1840.

Proof of the hitherto undemonstrated fundamental theorem of invariants, *Philosophical Magazine*, 1878.

On a point in the theory of vulgar fraction, *Amer. Jour. of Math*, 1880.

On Farey Series, Johns Hopkins University Circulars, 1883.

Answer on page 697.

COMPUTER SCIENCE SAMPLER

Edited by: **Catherine C. McGeoch**

Zero-Knowledge Proofs

Catherine C. McGeoch

On a moonless night the spy returns to the castle after a reconnoitering mission to the enemy camp. As he nears the gate a voice whispers, "What's the password?" But is it friend or foe who whispers? How can the spy show that he knows the password without actually revealing it to a possible imposter?

The spy's dilemma is commonplace now with the widespread use of telecommunications. When your automatic teller machine communicates with your bank, each must be assured that the other is legitimate; the electronic "passwords" must be unforgeable and must be of no use to imposters and eavesdroppers. One method that has been proposed for exchanging passwords in this context is the *zero-knowledge proof*.

Renaissance mathematicians developed their own primitive zero-knowledge proof systems. When both Tartaglia and Fior claimed knowledge of an algebraic solution to cubic equations, a contest was arranged in which each proposed thirty problems for the other to solve. In the end, Tartaglia had solved all thirty, thus providing a convincing demonstration that he knew the method without actually revealing it. Fior solved none. (It turned out that each had worked out solutions to certain classes of cubics, but neither had solved the general problem [2]).

We've progressed considerably in formalizing this idea. An *interactive protocol* comprises two algorithms P (the prover) and V (the verifier) that read a common *input string* w of length $|w|$ and then compute and communicate in alternating turns to determine whether w has some specified property. The verifier is *polynomially-bounded*: it must eventually halt and its total computation time must be bounded by a fixed polynomial in $|w|$. When it halts, the verifier outputs either *accept* or *reject* depending upon whether the property holds for w. The verifier is *probabilistic*, that is, allowed to make random choices during the computation according to the results of coin tosses. The prover is allowed to have unlimited computational power.

A *language* $\mathscr{L}$ is a set of strings. An *interactive proof system for* $\mathscr{L}$ is an interactive protocol in which P helps V to decide whether $w \in \mathscr{L}$. We require that with high probability the verifier be correct when accepting or rejecting the membership of w in $\mathscr{L}$. More precisely, for every constant $c > 0$, for sufficiently large $w \in \mathscr{L}$ the probability (over all coin tosses) that V halts and accepts must be at least $1 - |w|^{-c}$. If $w \notin \mathscr{L}$ then we require that no prover P^* be able to convince V otherwise: that is, for every $c > 0$ and large enough w, and for any interactive protocol (P^*, V), V rejects with probability at least $1 - |w|^{-c}$.

In a *zero-knowledge* interactive proof system, whenever $w \in \mathscr{L}$, P reveals no additional knowledge beyond the fact of membership. Informally, "no additional knowledge" means that the computational power of any verifier V^* after participating in the protocol is no more than what V^* would have gained by simply assuming $w \in \mathscr{L}$.

To solve the spy's dilemma we use an interactive zero-knowledge proof, choosing $\mathscr{L}$, w and a "secret" concerning w. An authentic P will transmit parts of the secret so that V accepts $w \in \mathscr{L}$, but the transmission is otherwise useless to eavesdroppers and bogus verifiers. An imposter P^* would, with high probability, cause V to reject w.

Let $\mathscr{L}_3$ be "the set of strings that represent 3-colorable graphs" under some fixed graph-representation scheme. A graph is 3-colorable if its vertices can be assigned colors such that no adjacent vertices have the same color and no more than 3 colors are used. Let the set of colors be denoted $\mathscr{C}$. Both P and V have access to an *encryption function* $f\colon (\mathscr{C} \times \mathscr{R}) \to \mathscr{C}^{\mathscr{C}}$, where $\mathscr{R}$ contains long strings of h and t values (representing long sequences of coin tosses) and $\mathscr{C}^{\mathscr{C}}$ is a set of encrypted colors.

The common input string w_G represents a particular 3-colorable graph G of n vertices and m edges. The secret, known only to P, is a correct 3-coloring of G; let c_i denote the color of vertex i under this coloring. An interactive zero-knowledge proof that $w_G \in \mathscr{L}_3$ is sketched below.

1. P applies a random permutation π to the colors: now each vertex i has color $\pi(c_i)$. Next, for each $i = 1 \ldots n$, the prover forms a random string r_i from several coin tosses and computes $c_i^e = f(\pi(c_i), r_i)$. The encrypted vertex colors c_i^e are sent to V.
2. V saves $c_1^e \ldots c_n^e$ and then chooses two adjacent vertices x and y at random and sends them to P.
3. P checks that (x, y) is really an edge in G. If not, the prover stops, having detected an imposter V that doesn't know the protocol. If (x, y) is an edge, the prover sends the colors $\pi(c_x)$ and $\pi(c_y)$ and the values r_x and r_y to V.
4. V computes $c'_x = f(\pi(c_x), r_x)$ and $c'_y = f(\pi(c_y), r_y)$ and looks for inconsistencies with the transmission in Step 1, checking that $c'_x = c_x^e$ and $c'_y = c_y^e$. The verifier also looks for violations of 3-colorability, checking that $\pi(c_x), \pi(c_y) \in C$ and that $\pi(c_x) \neq \pi(c_y)$. If any one of these checks fails, then V stops and rejects.
5. If the checks all pass, then P and V begin again in Step 1. If m^2 iterations of this protocol are completed without rejection, then V halts and accepts w_G.

Certainly the above protocol represents an interactive proof system for $\mathscr{L}_3$. If $w_G \in \mathscr{L}_3$ then V accepts with probability 1 after m^2 iterations. If $w_G \notin \mathscr{L}_3$ then the prover must send an invalid coloring (one with adjacent vertices the same color or one that uses more than 3 colors) in Step 1, which will be detected in Step 4 with probability at least $1/m$ at each iteration. The probability that V halts and rejects after m^2 random probes is at least $1 - (1 - 1/m)^{m^2}$. A little calculation shows that this probability is sufficient (with the reasonable assumptions that $|w| \leq 2m \log_2 n$ and there are no isolated vertices in G).

Indeed, for an interactive proof it would be sufficient for P simply to send the vertex colors to V; the extra steps are needed to ensure zero-knowledge. In Step 4, V "learns" that vertices x and y have different colors, which is no more than it

would learn from simply assuming $w_G \in \mathscr{L}_3$. The verifier gains no additional knowledge over time because the colors are randomly permuted and encrypted at each iteration. Even after several probes V has no idea how to 3-color the graph. A formal proof of zero-knowledge is rather too long to go into here: see Goldreich et al. [4] [5] for details.

BUT WILL IT WORK? Some nagging details must be addressed if this protocol is to be of any use to our spy. First, the proof of zero-knowledge depends upon an assumption that $f(\cdot, \cdot)$ is a *secure encryption* scheme, in the sense that it is not feasible to decrypt by deriving each $\pi(c_i)$ from c_i^e. Such a function is not known to exist.

Second, we must be assured that only the legitimate prover P could know a correct 3-coloring of G. The problem of finding 3-colorings of arbitrary graphs is known to be *NP-Hard*: as a consequence it is widely believed (but not proven) that any algorithm for finding 3-colorings must use exponential time on some graphs. Suppose we could build G such that the coloring is known by construction, but finding it independently requires time exponential in the size of G. Then we could secretly tell the coloring to P and (by choosing G large enough) be assured that any impostor computer would need, say, 10,000 years to find a 3-coloring. We also would have settled the most important open question in complexity theory today by proving that a famous set of problems known as $\mathscr{NP}$ is not equivalent to another set called $\mathscr{P}$.

So our zero-knowledge scheme is not provably secure. Even without this assurance, however, the method is efficient and reliable enough to have been applied in practice. There are several encryption functions that have not been broken. A well-known one, for example, encrypts by multiplying large primes and relies on the fact that there is no known way to factor large numbers efficiently. And we can take other steps to reduce the chance of compromising the protocol: there exist zero-knowledge proofs that do not require encryption functions at all, and there exist problems that are "harder" than 3-coloring to solve.

FURTHER READING. The notions of interactive proof systems and knowledge complexity of proofs were first developed by Goldwasser et al. [6], [7]. Blum et al. [1] have since shown that zero-knowledge does not require interaction: that is, any interactive zero-knowledge proof can be replaced by one in which P sends messages to V but never receives any.

Goldreich et al. [4], [5] give several examples of zero-knowledge proofs, including the 3-colorability problem shown here, and discuss issues relating to secure protocols. Landau [8] describes what can happen when mathematicians and theoretical computer scientists get involved with problems of interest to the Department of Defense.

Technically, the zero-knowledge proof we've seen does reveal one bit of knowledge, namely that $w \in \mathscr{L}$. Fiege, Fiat and Shamir [3] have exhibited proofs that are truly zero-knowledge: the prover proves that he knows whether or not $w \in \mathscr{L}$, but doesn't even reveal that fact. Perhaps someday we can extend zero-knowledge protocols to achieve a complete standstill of mathematical progress such as that attempted during the Renaissance. For example, maybe I could

demonstrate knowledge of the status of Fermat's last theorem[1] without revealing the proof or even the truth or falsehood of the statement. Heaven forbid.

REFERENCES

1. M. Blum, P. Feldman, and S. Micali, Non-interactive zero-knowledge and its applications, *Proceedings of the 29th Symposium on Foundations of Computer Science*, 1988, pp. 103–112.
2. C. B. Boyer, *A History of Mathematics*, Wiley and Sons, 1968.
3. U. Feige, A. Fiat, and A. Shamir, Zero knowledge proofs of identity, *Proceedings of the 19th Symposium on Theory of Computing*, 1987, pp. 210–217.
4. O. Goldreich, S. Micali, and A. Widgerson, Proofs that yield nothing but their validity and a methodology of cryptographic protocol design, *Proceedings of the 27th Symposium on Foundations of Computer Science*, 1986, pp. 174–187.
5. O. Goldreich, S. Micali, and A. Widgerson, Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proofs, *Journal of the Association for Computing Machinery*, (38) 1, 1991, pp. 691–729.
6. S. Goldwasser, S. Micali, and C. Rackoff, The knowledge complexity of interactive proof systems, *Proceedings of the 17th Symposium on Theory of Computing*, 1985, pp. 291–304.
7. S. Goldwasser, S. Micali, and C. Rackoff, The knowledge complexity of interactive proof systems, *SIAM J. Computing* (18) 1, February 1989, pp. 186–208.
8. S. Landau, Zero knowledge and the Department of Defense, *Notices of the AMS* (35) 1, January 1988, pp. 5–12.

Department of Mathematics and Computer Science
P.O. Box 2239
Amherst College
Amherst, MA 01002
ccm@cs.amherst.edu

PROBLEMS FOR SOLUTION

E. 36 *Proposed by B. H. Brown, Dartmouth College.*
Show that the thirteenth of the month is more likely to be Friday than any one of the other days of the week.

—*American Mathematical Monthly* 40, (1933) p. 295

[1]Please substitute "Goldbach's Conjecture" for "Fermat's Last Theorem" here.

PROBLEMS AND SOLUTIONS

Edited by:
Richard T. Bumby, Fred Kochman and Douglas B. West

Proposed problems should be sent to the MONTHLY PROBLEMS address given on the inside front cover. Please include solutions, relevant references, etc. Three copies are requested.

Solutions of published problems should arrive before February 28, 1994 at the MONTHLY PROBLEMS address given on the inside front cover. Solutions should be typed with double spacing, including the problem number and the solver's name and mailing address. Two copies suffice. A self-addressed postcard or label should be included if an acknowledgment is desired.

*An asterisk (*) after the number of a problem, or part of a problem, indicates that no solution is currently available. Partial solutions will be useful in such cases. Otherwise, the published solution is likely to be based on a solution which is complete and correct. Of course, an elegant partial solution or a method leading to a more general result is always useful and welcome. In addition, references to other appearances of MONTHLY problems or to solutions of these problems in the literature are also solicited.*

PROBLEMS

10322. *Proposed by Jiang Huanxin, student, FuDan University, ShangHai, China*

Let $ABCD$ and $AEFG$ be squares with the common vertex A and *different* edge lengths. Let $\theta = \angle EAD$ $(0 < \theta < \pi/2)$. Suppose that EF and CD intersect at the point P. For which value of θ will AP be perpendicular to CF?

10323. *Proposed by David E. Penney and Carl Pomerance, University of Georgia, Athens, GA.*

For a natural number n, let $t(n)$ be the sum of the divisors d of n in the range $1 \le d < n$ with n/d being squarefree. Is there an integer n for which the sequence $n, t(n), t(t(n)), \ldots$ is unbounded?

10324. *Proposed by William P. Wardlaw, United States Naval Academy, Annapolis, MD.*

Let a and m be positive integers and define the sequence $\langle x_n \rangle$ by $x_0 = 1$ and $x_{n+1} = a^{x_n}$. Show that there is a positive integer N such that $x_h \equiv x_k \pmod{m}$ whenever $N \le h \le k$.

10325. *Proposed by Broderick Oluyede, Georgia State University, Atlanta, GA.*

For $i = 1, 2, \ldots, r$ and $j = 1, 2, \ldots, c$, let $p_{i,j} \geq 0$, and assume that $\Sigma_{i=1}^{r}\Sigma_{j=1}^{c} p_{i,j} = 1$. Define $p_{i,\cdot} = \Sigma_{j=1}^{c} p_{i,j}$ and $p_{\cdot,j} = \Sigma_{i=1}^{r} p_{i,j}$. In addition, suppose that

$$p_{i+1,j+1} \sum_{h=1}^{i} \sum_{k=1}^{j} p_{h,k} \geq \sum_{h=1}^{i} p_{h,j+1} \sum_{k=1}^{j} p_{i+1,k}$$

for $0 < i < r$ and $0 < j < r$. Prove that

$$\sum_{h=1}^{i} \sum_{k=1}^{j} p_{h,k} \geq \sum_{h=1}^{i} p_{h,\cdot} \sum_{k=1}^{j} p_{\cdot,k}$$

for $0 < i < r$ and $0 < j < r$.

10326. *Proposed by Ira Gessel, Brandeis University, Waltham, MA.*

For r a positive integer, let K_r be the smallest positive integer such that

$$\frac{K_r}{n+r}\binom{2n}{n}$$

is an integer for all $n \geq 0$. Show that

$$K_r = \frac{r}{2}\binom{2r}{r}.$$

10327. *Proposed by Jerome Minkus, Berkeley, CA.*

Find the simple continued fraction for $(e + 3)/4$.

10328. *Proposed by A. Keith Austin, The University of Sheffield, Sheffield, England.*

Let A and B be sets such that $A \cap B = \varnothing$ and $A \cup B$ is the unit square $[0,1] \times [0,1]$. Prove or disprove the following:

(a)* Either there is a continuous function f: $[0,1] \to A$ with $f(0) = (0, y_0)$ for some y_0 and $f(1) = (1, y_1)$ for some y_1, or there is a continuous function g: $[0,1] \to B$ with $g(0) = (x_0, 0)$ for some x_0 and $g(1) = (x_1, 1)$ for some x_1.

(b) f and g as in part a cannot both exist.

10329. *Proposed by Gérard Letac, Université Paul Sabatier, Toulouse, France.*

Let $f(x)$ is a positive continuous function defined for $0 < x < 1$ such that, for all u with $0 < u < 1$, one has $\int_u^1 f(x)f(u/x)\,dx = u^{1/2}$. Prove that

$$f(x) = \sqrt{\frac{2x}{\pi(1-x^2)}}\,.$$

NOTES

Notes: (10323) A related sequence, called the *aliquot sequence* of n is generated by using a function $s(n)$ which is the sum of all divisors d of n in the interval $1 \leq d < n$. Some examples of aliquot sequences are: 9, 4, 3, 1, 0, 0, ...; 6, 6, ...; and 220, 284, 220, ... It is unkown whether all aliquot sequences are eventually periodic; the case of $n = 276$ is unresolved at this time. **(10327)** The standard reference for continued fractions is 0. Perron, *Die Lehre von den Kettenbrüchen*. The fourth chapter describes the continued fraction for e and related "Hurwitz continued fractions".

SOLUTIONS

Uniqueness from Asymptotic Behavior

E 3449 [1991, 553]. *Proposed by Mark A. Pinsky, Northwestern University, Evanston, IL.*

Suppose s is a continuous real-valued function on $[0, +\infty)$ such that s is differentiable on $(0, +\infty)$, $0 \leq s(t) \leq t^2$, and

$$\frac{ds}{dt} = t + \sqrt{t^2 - s} \quad (t > 0).$$

Prove that s is unique and obtain a closed formula for s.

Solution I by J. B. Thoo, student, University of California, Davis, CA. By direct substitution it is easily verified that $s(t) = \frac{3}{4}t^2$ satisfies the requirements.

To establish that this $s(t)$ is the unique solution, we will show that any two solutions $s_1(t)$ and $s_2(t)$ must be identical. Let us define $g(t) = (s_1(t) - s_2(t))^2$, which is clearly non-negative. Then for all $t > 0$,

$$\begin{aligned} g'(t) &= 2(s_1(t) - s_2(t))(s_1'(t) - s_2'(t)) \\ &= -2\frac{(s_1(t) - s_2(t))^2}{(t^2 - s_1(t))^{1/2} + (t^2 - s_2(t))^{1/2}} \\ &\leq 0. \end{aligned}$$

Hence, $g(t) \leq g(0)$ for all $t > 0$. But since $0 \leq s(t) \leq t^2$ implies $s_1(0) = 0$ and $s_2(0) = 0$, then also $g(0) = 0$; hence, for all $t > 0$, $g(t) \leq 0$. Since g is both a non-negative function and, it now appears, a non-positive one as well, it must be identically zero, and so therefore $s_1 = s_2$, as claimed.

Solution II by Frédéric Brulois, California State University-Dominguez Hills, Carson, CA. Re-write the given condition in the form $s'(t) - t = (t^2 - s(t))^{1/2}$. Square it and differentiate it to obtain $2(s'(t) - t)s''(t) = s'(t)$. This is a first-order

homogeneous equation in $s'(t)$, which can be solved by standard techniques to obtain $s'^2(t)(3t - 2s'(t)) = C$. Thus, using the parameter $p = s'(t)$, we get $t = (2/3)p + (C/3)p^{-2}$ and $s = (1/3)p^2 + (2C/3)p^{-1}$. Since $s'(t)$ lies between t and $2t$ for all $t > 0$, the only possible value of C that would permit this equation to hold for arbitrarily small t is 0. It follows from the parametric solution that $t = 2p/3$ and $s = p^2/3$. Thus $s(t) = 3t^2/4$.

Solution III by Kiran S. Kedlaya, student, Harvard University, Cambridge, MA. Define $f(x) = \frac{1}{2}(1 + (1 - x)^{1/2})$, and note that $x = 3/4$ is a fixed point of this function. Also note that $|f'(x)| < 7/8$ for $1/2 < x < 7/8$ and that this interval is taken into itself by f. Furthermore, any sequence defined inductively by $x_{n+1} = f(x_n)$, with $x_0 \in [0, 1]$, eventually enters this attracting basin and converges to $3/4$. In particular, we choose $x_0 = 0$.

We prove by induction that $x_{2n}t^2 \leq s(t) \leq x_{2n+1}t^2$ for all t and all n. From this and the fact that $x_n \to 3/4$, we may conclude that $\frac{3}{4}t^2 \leq s(t) \leq \frac{3}{4}t^2$, and thence that $s(t) = \frac{3}{4}t^2$.

The statement with $n = 0$ is hypothesized, so let us show that if $x_{2k}t^2 \leq s(t) \leq x_{2k+1}t^2$ holds for some $k \geq 0$, then $x_{2k+2}t^2 \leq s(t) \leq x_{2k+3}t^2$ holds also. We have

$$2tx_{2k+2} = t + \sqrt{t^2 - x_{2k+1}t^2} \leq t + \sqrt{t^2 - s} \leq t + \sqrt{t^2 - x_{2k}t^2} = 2tx_{2k+1}$$

where the equalities follow from the inductive definition of x_n and the inequalities follow from the induction hypothesis. Then by integrating, we obtain

$$\int_0^t 2tx_{2k+2}\,dt \leq \int_0^t s'(t)\,dt \leq \int_0^t 2tx_{2k+1}\,dt$$

$$x_{2k+2}t^2 \leq s(t) \leq x_{2k+1}t^2,$$

where we have used the fact that $s(0) = 0$. Then, by similar reasoning, we reach the desired conclusion that

$$x_{2k+2}t^2 \leq s(t) \leq x_{2k+3}t^2.$$

Editorial comment. These three solutions are representatives of the principal methods of solution. These may be summarized as follows.

Method I: Guess the answer. Prove that it works. Then give careful attention to proving uniqueness.

Method II: Transform the differential equation by a change of variable or further differentiation into an equation whose complete solution can be found by standard methods. Then impose the restriction that $0 \leq s(t) \leq t^2$.

Method III: Use the differential equation to iteratively produce explicit refinements of the requirement that $0 \leq s(t) \leq t^2$ for all $t > 0$. Existence and uniqueness will then follow from general fixed-point arguments. In this method, a familiar method of proof of the existence and uniqueness theorem of differential equations is applied, exploiting a global inequality on the solution to control $\int_0^t s'(t)\,dt$.

Solved by 55 readers, some submitting more than one solution, and the proposer. This yielded 21 solutions by Method I, 19 by Method II, 16 by Method III, and 4 hybrids. In addition there were 7 submissions found to be incomplete or inaccurate.

Graceful Permutations

E 3455 [1991, 646]. *Proposed by D. G. Rogers, University of Aberdeen, Scotland, and Howard University, Washington, DC.*

It is known that if $n \equiv 0 \pmod 4$ or $n \equiv 1 \pmod 4$, then there exist permutations $(x_1, x_2, \ldots, x_n)$ of $(1, 2, \ldots, n)$ such that the differences $|x_k - k|$, $1 \le k \le n$, are all distinct. (Cf. E 3269 [1988, 554; 1989, 843].) Prove that the number of such permutations is a multiple of 4.

Solution by M. Roth and O. Šuch, Queen's University, Kingston, Ontario, Canada. Let S be the set of permutations such that the specified differences are all distinct. Let $n > 1$ to assure that the identity does not belong to S. We show that the number of such permutations is a multiple of 4 by defining two involutions π and ρ on S such that $\pi\rho(\sigma) = \rho\pi(\sigma)$ and $\pi(\sigma) \neq \rho(\sigma)$ for any $\sigma \in S$. If we also show that π and ρ do not fix any element of S then the action of these operations splits S into disjoint orbits of size 4, which proves $|S| \equiv 0 \pmod 4$.

Letting $\sigma = x_1, \ldots, x_n$, $\pi(\sigma) = y_1, \ldots, y_n$ and $\rho(\sigma) = z_1, \ldots, z_n$, we define $\pi(\sigma)$ and $\rho(\sigma)$ explicitly by $y_k = j$ if and only if $x_j = k$, and $z_k = j$ if and only if $x_{n+1-k} = n + 1 - j$. By construction, these produce permutations, preserve the set of differences, and are involutions. Note that π takes a permutation to its inverse. An element of S cannot interchange a pair of points, and can have at most one fixed point, so π fixes no element of S. If $\rho(\sigma) = \sigma$, then $x_k = j$ if and only if $x_{n+1-k} = n + 1 - j$, in which case the differences for positions k and $n + 1 - k$ have the same magnitude and $\sigma \notin S$.

By direct calculation, both $\pi\rho(\sigma)$ and $\rho\pi(\sigma)$ have $n + 1 - k$ in position $n + 1 - j$ if and only if $x_k = j$, so $\pi\rho = \rho\pi$. All that remains to be shown is that these maps are not equal on any member of S. Note that $\rho(\sigma)$ has $n + 1 - x_{n+1-k}$ in position k. If $\pi(\sigma) = \rho(\sigma)$, then σ also has k in position $n + 1 - x_{n+1-k}$. This makes the absolute difference between a position and its value the same at position $n + 1 - k$ and position $n + 1 - x_{n+1-k}$. If $\sigma \in S$, the differences are distinct for distinct positions, and hence $k = x_{n+1-k}$ for all k. This is satisfied only by permutation which is not in S.

Editorial comment. Only a few solvers made explicit mention of the fact that the statement of the problem needed to be modified to require $n > 1$. The term "graceful" for the permutations with this property was suggested by Albert Nijenhuis.

Solved also by D. Callan, R. J. Chapman (U.K.), P. Čižek (student, Czech Republic), M. Dindos (Slovakia), J. Fukuta (Japan), L. L. Gardner, R. High, A. A. Jagers (The Netherlands), I. Kastanas, K. S. Kedlaya (student), O. P. Lossers (The Netherlands), J. H. Nieto (Venezuela), A. Nijenhuis, J. H. Steelman, C. Voas, National Security Agency Problems Group, Shreveport Problem Solving Group (LSU), and the proposer.

A Variant of the Erdős-Faber-Lovász Conjecture

6664 [1991, 655]. *Proposed by Paul Erdős, Hungarian Academy of Sciences, Budapest*

Let G be a graph whose edges can be covered by n complete subgraphs with n vertices each (i.e., G is the union of n copies of K_n, with no restrictions on shared vertices).

(a) Prove that the chromatic number of G is less than $1 + n\sqrt{n-1}$.

(b) Prove that this bound is asymptotically best possible, i.e., if $f(n)$ is the maximum chromatic number of a graph constructed in this way, then $f(n) = \{1 + o(1)\}n^{3/2}$.

Solution of (a) by Ilias Kastanas, California State University, Los Angeles, CA, and by Charles Vanden Eynden, Illinois State University, Normal, IL (independently). A graph with chromatic number k has at least $\binom{k}{2}$ edges, because if there is no edge between the set of vertices of color i and the set of vertices of color j, then colors i and j can be combined into a single color. On the other hand, G has at most $n\binom{n}{2}$ edges, and the inequality $k(k-1) \leq n^2(n-1)$ implies $k < 1 + n\sqrt{n-1}$.

Solution of (b) by Richard Holzsager, American University, Washington, DC. Consider the affine plane of order p, where p is a prime. There are p^2 points and $p^2 + p$ lines of size p, such that each pair of points appears in a unique line. If we view these lines as cliques (complete graphs) on the points, then we have expressed the complete graph K_{p^2} as a union of $p^2 + p$ cliques of size p. We now expand each point into a clique of $p + 1$ points to express $K_{p^3+p^2}$ as a union of $p^2 + p$ cliques of size $p^2 + p$. Hence $f(p^2 + p) \geq p^3 + p^2 = (1 + o(1))(p^2 + p)^{3/2}$.

Now, let n be arbitrary, and fix $\varepsilon > 0$. By the prime number theorem, the number of primes below x is eventually greater than the number of primes less than $(1-\varepsilon)x$, meaning there are primes between $(1-\varepsilon)x$ and x, if x is large enough. Taking n large enough and $x = \sqrt{n + 1/4} - 1/2$, we obtain a prime p with $(1-2\varepsilon)n < p(p+1) < n$. Therefore, $f(n) \geq f(p^2 + p) \geq (1 + o(1))(p^2 + p)^{3/2} = (1 + o(1))n^{3/2}$.

Editorial comment. This problem was first received from the proposer by the editors in 1987. In 1988, P. Horák heard of the problem and found a solution, which was published as "A coloring problem related to the Erdős-Faber-Lovász conjecture," *J. Combinatorial Theory*, Ser. B 50 (1990), 321–322.

Suppose we add the constraint that each edge of G appears in exactly one clique (note that this is violated by the construction in (b)). The Erdős-Faber-Lovász conjecture is that in this case the chromatic number is exactly n.

Zoltan Füredi improved the upper bound of (a) when n is of the form $q^2 + q$. He proved that $q^3 + q^2$ is an upper bound in this case, which makes the projective plane construction of (b) optimal when $n = q^2 + q$ and q is a prime power.

The problem was completely solved by all three solvers cited above. Solutions were also given by the proposer and by Z. Füredi.

More Pigeons on the Circle

E 3463 [1991, 852]. *Proposed by Donald E. Knuth, Stanford University, Stanford, CA.*

Let S be a set of m distinct points on the unit circle such that no two are diametrically opposite. For a fixed integer $n \leq m/2$, suppose that we mark every point p in S such that fewer than n of the remaining points in S lie in the semicircle counterclockwise from p. Prove that at most n points are marked.

Solution by John H. Lindsey II, Fort Myers, FL. Fix n and delete unmarked points one by one, each time allowing unmarked points to become marked as the semicircles empty out, until only $2n$ points remain or all remaining points are marked. At this time a point is marked only if the nth point later is more than a

semicircle away. If that point is also marked, then traversing $2n$ points travels more than the full circle, which happens only if fewer than $2n$ points remain. Hence the stopping condition occurs when exactly $2n$ points remain, and the marked points consist of exactly one point from each pair of points separated by $n-1$ points in each direction. This implies there were at most n marked points in the original set.

Solved by 26 other readers and the proposer.

A Half Step Towards Carmichael's Conjecture

6671 [1991, 862]. *Proposed by Carl Pomerance, University of Georgia, Athens, GA.*

Let $V(x)$ denote the number of distinct values not exceeding x taken on by Euler's arithmetical function ϕ. Let $V^*(x)$ denote the number of these values with a unique pre-image. For example, $V(15) = 7$, $V^*(15) = 0$.

R. D. Carmichael conjectured that $V^*(x) = 0$ for all x. Prove the weaker assertion that $\liminf_{x\to\infty}\{V^*(x)/V(x)\} < 1$.

Solution by L. E. Mattics, University of South Alabama, Mobile, AL. Let $\varepsilon = 2^{1/2} - 1$ and let $V_0(x)$ be the number of values of $\phi(w)$ not exceeding x such that w is odd. We will show that we can prove that $\liminf_{x\to\infty} V^*(x)/V(x) \le 2^{-1/2}$ regardless of whether or not the following proposition holds.

Proposition. *For every positive integer N there is an $x \ge N$ such that $V_0(x/2) > \varepsilon V(x)$.*

If the proposition does hold then there are arbitrarily large x such that

$$V\left(\frac{x}{2}\right) \ge V_0\left(\frac{x}{2}\right) + V^*\left(\frac{x}{2}\right) \ge \varepsilon V(x) + V^*\left(\frac{x}{2}\right) \ge (\varepsilon+1)V^*\left(\frac{x}{2}\right) \ge 2^{1/2}V^*\left(\frac{x}{2}\right)$$

so $\liminf_{x\to\infty} V^*(x)/V(x) \le 2^{-1/2}$.

Assume from now on that the proposition does not hold. Then there is an integer N such that for all $x \ge N$, $V_0(x/2) \le \varepsilon V(x)$. If $(2,u) = 1$ and $\phi(2^a u) \le x$ has only one pre-image, then $a \ge 2$ and $\phi(u) \le x/2^{a-1}$; and if v is odd and $\phi(u) = \phi(v)$, then $\phi(2^a u) = \phi(2^a v)$, so $u = v$. This implies that $V^*(x) \le \sum_{a=2}^{\infty} V_0(x/2^{a-1})$ where $V_0(c) = 0$ if $c < 1$.

Now let $m = \lfloor \log_2(x/N) \rfloor + 1$ then

$$\begin{aligned} V^*(x) &\le \sum_{a=2}^{m} \varepsilon^{a-1} V(x) + \sum_{a=m+1}^{\infty} V_0\left(\frac{x}{2^{a-1}}\right) \\ &\le \frac{\varepsilon}{1-\varepsilon} V(x) + \left(V_0(N) + V_0\left(\frac{N}{2}\right) + \cdots\right). \end{aligned}$$

Since $V(x) \to \infty$ as $x \to \infty$ and N is fixed we have $\liminf_{x\to\infty} V^*(x)/V(x) \le 2^{-1/2}$.

Editorial comment. All solutions provided an upper bound on the quantity $\liminf_{x\to\infty}\{V^*(x)/V(x)\}$. The best value obtained to date was $1/2$, which was given by the proposer. All solutions considered the set $\Phi_o = \{m\colon m = \phi(2k+1)$ for some $k\}$, and noted that, if m is $\phi(n)$ for some n, then there is an integer h

with $m/2^h \in \Phi_o$. This should be compared to problem E 3661 [1990, 63; 1991, 443] in which examples of $\phi(n) \notin \Phi_o$ were given.

Solved also by I. Kastanas and the proposer.

Consecutive Convergents

10187 [1992, 60]. *Proposed by Irving Adler, North Bennington, VT.*

Suppose n_{k-1}/d_{k-1} and n_k/d_k are consecutive convergents of the simple continued fraction for some real number α in (0, 1). Assume you are given only the values of d_{k-1} and d_k. Construct an algorithm for determining the values of n_{k-1} and n_k.

Solution by Nicholas C. Singer, Annandale, VA. The problem as stated has two possible solutions, because the convergents to α and $1-\alpha$ have essentially the same sequence of denominators. That is, if $0 < \alpha < 1/2$, then α has the continued fraction expansion $\alpha = [0, a_1, a_2, a_3, \dots]$ with $a_1 \geq 2$; and then $1 - \alpha = [0, 1, a_1 - 1, a_2, a_3, \dots]$. Using the standard recurrence relation

$$d_k(\alpha) = a_k d_{k-1}(\alpha) + d_{k-2}(\alpha), \quad d_{-2}(\alpha) = 1, d_{-1}(\alpha) = 0,$$

we conclude that for $k \geq 1$, $d_k(1-\alpha) = d_{k-1}(\alpha)$. We need exactly one bit of additional information to get a unique answer: (i) is α greater than or less than 1/2? or (ii) what is the parity of k?

It is immediate, using the recurrence relations, that $d_k/d_{k-1} = [a_k, a_{k-1}, a_{k-2}, \dots, a_1]$. The quotients and convergents are calculated using the usual continued fraction (which is equivalent to the Euclidean algorithm). The n_k satisfy the same recurrence as the d_k with the initial conditions replaced by $n_{-2} = 0$, $n_{-1} = 1$. In addition, $n_0 = a_0 = 0$ so we also have $n_k/n_{k-1} = [a_k, a_{k-1}, a_{k-2}, \dots, a_2]$. (The case $k = 1$ is special since $n_0 = 0$.) That is, we take n_k and n_{k-1} to be the numerator and denominator of the penultimate convergent of the continued fraction expansion of d_k/d_{k-1}.

The usual application of the Euclidean algorithm always gives $a_1 \geq 2$. However, $[a_k, a_{k-1}, a_{k-2}, \dots, a_2, a_1] = [a_k, a_{k-1}, a_{k-2}, \dots, a_2, a_1 - 1, 1]$, which leads to the alternative expansion $n_k/n_{k-1} = [a_k, a_{k-1}, a_{k-2}, \dots, a_2, a_1 - 1]$. This corresponds to $1 - \alpha = [0, 1, a_1 - 1, a_2, \dots, a_k, \dots] > 1/2$. This expansion of n_k/n_{k-1} has k convergents, whereas the previous expansion had $k - 1$. Hence knowing the answer to either question (i) or question (ii) allows us to produce the unique correct result.

Solved also by D. Callan, R. J. Chapman (U. K.), D. Chinitz (student), C. H. Ebersole, B. Haible (Germany), R. J. Hendel, R. High, O. P. Lossers (The Netherlands), A. Nijenhuis, J. H. Steelman, R. Stong, B. M. M. de Weger (The Netherlands), E. A. Weinstein, O. Wyler, Anchorage Math Solutions Group, National Security Agency Problems Group, and the proposer.

Complex Conjugation of $\mathbb{C}(z)$

10191 [1992, 61]. *Proposed by Dragomir Ž. Đoković, University of Waterloo, Waterloo, Ontario, Canada.*

Let G be the group of $\mathbb{C}$-automorphisms of the function field $\mathbb{C}(z)$ and Σ the set of involutory automorphisms of $\mathbb{C}(z)$ which extend the complex conjugation on

$\mathbb{C}$. Show that Σ splits into two orbits under the action $G \times \Sigma \to \Sigma$, $(\alpha, \beta) \mapsto \alpha \circ \beta \circ \alpha^{-1}$. (Thus there are only two essentially different ways of extending the complex conjugation to an involutory automorphism of $\mathbb{C}(z)$.)

Solution by Robin J. Chapman, University of Exeter, Exeter, U.K. It is well known that if $\alpha \in G$ then α is determined by $\alpha(z) = (az + b)/(cz + d)$ where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a non-singular matrix over $\mathbb{C}$. Two different choices of A give the same α if and only if they are scalar multiples of each other. Also, composition in G corresponds to matrix multiplication. Furthermore, an automorphism β of $\mathbb{C}(z)$, restricting to conjugation on $\mathbb{C}$, is also determined by $\beta(z) = (pz + q)/(rz + s)$ where $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is a non-singular matrix over $\mathbb{C}$; and again, two different B give the same β if and only if they are scalar multiples. Now we easily compute that $\beta^2(z) = (tz + u)/(vz + w)$ where $C = \begin{pmatrix} t & u \\ v & w \end{pmatrix} = \bar{B}B$. Hence $\beta \in \Sigma$ if and only if $\bar{B}B = \lambda I$ for some $\lambda \in \mathbb{C}$. If $\beta \in \Sigma$ then $\lambda^2 = \det \bar{B} \det B = |\det B|^2$. Hence $\lambda = \pm |\det B|$. As replacing B by μB changes λ to $|\mu|^2\lambda$ and $|\det B|$ to $|\mu|^2 |\det B|$ then the sign of λ is an invariant of β. If $B = \begin{pmatrix} 0 & 1 \\ \pm 1 & 0 \end{pmatrix}$ then $\bar{B}B = \pm I$ and so both signs occur. Call β positive or negative according to the sign of λ.

I claim now that if $\alpha \in G$ and $\beta \in \Sigma$ then $\alpha \circ \beta \circ \alpha^{-1}$ is positive if and only if β is. If α and β are represented by the matrices A and B respectively then $\alpha \circ \beta \circ \alpha^{-1}$ is represented by $B' = \overline{A^{-1}}BA$. Now $\overline{B'}B' = A^{-1}\bar{B}\bar{A}\overline{A^{-1}}BA = A^{-1}\bar{B}BA = \lambda I$ and the claim follows. Hence Σ splits into at least two G-orbits.

Take $\beta \in \Sigma$. We may represent β by a matrix B with $\det B = -\operatorname{sgn}(\beta)$. Hence $\bar{B} = -(\det B)B^{-1}$ and $B = \begin{pmatrix} a & b \\ c & -\bar{a} \end{pmatrix}$ where $a \in \mathbb{C}$, $b \in \mathbb{R}$, $c \in \mathbb{R}$ and $|a|^2 + bc = \pm 1$. Now if $|\zeta| = 1$ and $A_1 = \begin{pmatrix} \zeta & 0 \\ 0 & \bar{\zeta} \end{pmatrix}$ then $B' = \overline{A_1^{-1}}BA_1 = \begin{pmatrix} \zeta^2 a & b \\ c & -\overline{\zeta^2 a} \end{pmatrix}$ so that by a suitable choice of ζ we may assume that $B' = \begin{pmatrix} a' & b' \\ c & -a' \end{pmatrix}$ where $a' \in \mathbb{R}$ and $\det B' = \pm 1$. Hence B' has characteristic polynomial $X^2 \pm 1$ and so there is a real matrix A_2 with $A_2^{-1}B'A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ if β is positive and $A_2^{-1}B'A_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ if β is negative. Hence if $A = A_1A_2$ then $\bar{A}^{-1}BA = \begin{pmatrix} 0 & 1 \\ \pm 1 & 0 \end{pmatrix}$ and so there are at most two G-orbits in Σ.

Editorial comment. Robin Chapman also provided a cohomological interpretation of the result. If we let $\Gamma = \operatorname{Gal}(\mathbb{C}/\mathbb{R})$, then Γ acts on $G \cong PGL_2(\mathbb{C})$ by conjugation and it is not hard to see that the elements of Σ correspond to 1-cocylces of Γ in G and that two elements of Σ correspond to cohomologous cocycles if and only if they lie in the same G-orbit. Hence the set of orbits corresponds to the set $H^1(\Gamma, G)$. Using the exact sequence of Γ-modules

$$1 \to \mathbb{C}^* \to GL_2(\mathbb{C}) \to PGL_2(\mathbb{C}) \to 1$$

a standard theorem of Galois cohomology (Jean-Pierre Serre, *Local Fields*, Springer-Verlag, 1978, X.5), shows that the connecting map δ: $H^1(\Gamma, G) \to H^2(\Gamma, \mathbb{C}^*)$ is an isomorphism. Now as Γ is cyclic, it is immediate that $H^2(\Gamma, \mathbb{C}^*) \cong \mathbb{R}^*/N(\mathbb{C}^*) \cong \{\pm 1\}$ where N: $\mathbb{C} \to \mathbb{R}$ is the norm map, and the result follows. More generally if we replace $\mathbb{R}$ and $\mathbb{C}$ by K and L where L/K is a quadratic extension with Galois group Γ then the corresponding result is that the G-orbits of Σ are in one-to-one correspondence with $H^1(\Gamma, G) \cong H^2(\Gamma, L^*) \cong K^*/N_{L/K}(L^*)$.

Now $H^2(\Gamma, L^*)$ is the relative Brauer group $\operatorname{Br}(L/K)$, and as $|L : K| = 2$ this can be interpreted as the set of equivalence classes of 1-dimensional Severi-Brauer

varieties over K split by L. These are the projective curves defined over K which become isomorphic to the projective line after base change to L. If $\beta \in \Sigma$ then the fixed field $L(z)^{\beta}$ is the function field of the corresponding Severi-Brauer variety. If $L = \mathbb{C}$ and $K = \mathbb{R}$ and if β is positive, then $\mathbb{C}(z)^{\beta} \cong \mathbb{R}(t)$, the function field of the projective line over $\mathbb{R}$; and if β is negative, then $\mathbb{C}(z)^{\beta} \cong \mathbb{R}(x, y | x^2 + y^2 + 1 = 0)$, the function field of the conic C with homogeneous equation $X_1^2 + X_2^2 + X_3^2 = 0$ which has no points defined over $\mathbb{R}$. Explicitly, if $\beta(z) = z$, then β is positive and $\mathbb{C}(z)^{\beta} = \mathbb{R}(z)$; while if $\beta(z) = -1/z$, then β is negative and $\mathbb{C}(z)^{\beta} = \mathbb{R}(x, y)$ where $x = (z - 1/z)/2$ and $y = i(z + 1/z)/2$ satisfy $x^2 + y^2 = -1$.

The proposer's proof that there are at most two orbits involved showing that any matrix B with $\bar{B}B = I$ can be written as $\overline{A^{-1}}A$, for which he referred to D. Ž. Đoković, "On some representations of matrices", *Linear and Multilinear Algebra*, 4 (1976), 33–40.

Solved also by D. Callan and the proposer.

Collaborating editors: *David F. Appleyard*, *Paul T. Bateman*, *Bruce C. Berndt*, *Duane M. Broline*, *Barry W. Brunson*, *Frank S. Cater*, *Gulbank D. Chakerian*, *Underwood Dudley*, *Gerald A. Edgar*, *Michael A. Filaseta*, *Ira M. Gessel*, *Richard A. Gibbs*, *Jerrold R. Griggs*, *Douglas A. Hensley*, *John R. Isbell*, *Mourad E. H. Ismail*, *Murray Klamkin*, *Daniel J. Kleitman*, *Frederick W. Luttmann*, *Frank B. Miles*, *Richard Pfiefer*, *Stephen L. Portnoy*, *J. O. Shallit*, *John Henry Steelman*, *Kenneth B. Stolarsky*, *David E. Tepper*, *Douglas B. Tyler*, *Daniel Ullman*, and *William E. Watkins*.

"You know, for a mathematician he did not have enough imagination. But he has become a poet and now he is doing fine....."

—*Hilbert* (*to Cassirer*, *about a former student*)

Answer to Picture Puzzle
(p. 661)
George Pólya.

Answer to Who Was the Author
(p. 681)
James Joseph Sylvester.

The American Mathematical Monthly

Volume 100, Number 8 / OCTOBER 1993

NOTICE TO AUTHORS

The *Monthly* publishes articles, notes, and other features about mathematics and the profession. The readership of the *Monthly* is intended to include everybody who is mathematically inclined, including of course professional mathematicians and students of mathematics at all collegiate levels. While no single article or feature is likely to appeal to everyone, material should interest and be accessible to a large number of readers. This is the most important criterion for acceptance.

Articles may be expositions of old results or presentations of new ones. They may concern all of mathematics or one small area, a broad development or a single application, historical reminiscences or one important event. While some articles may contain the author's new research, the novelty of material and generality of the results is far less important than the clarity of exposition and general interest. Discussing one illuminating case of a well known result is far better than providing all the details of an obscure but new proposition. Articles in the *Monthly* are supposed to inform and to entertain; they are meant to be read rather than archived.

Notes are short and possibly informal articles. A note may concern a clever new proof of an old theorem, a novel way to present tired material, or a lively discussion of a philosophical (but still mathematical) issue. Also, any topic is suitable, so long as it is related to mathematics. Because a note is short, the first few sentences are the most important part: They should explain the purpose and invite the reader in. Photographs or diagrams often will attract the reader's attention.

All articles and notes should be sent to the editor:

JOHN EWING,
Department of Mathematics,
Indiana University,
Bloomington, IN 47405.

Please send 3 copies, typewritten on only one side of the paper. Illustrations should be carefully drawn on separate sheets of paper in black ink; the original should be without lettering and two copies should have appropriate captions and lettering indicated.

Proposed problems or solutions should be sent to:

RICHARD BUMBY,
P.O. Box 10971
New Brunswick, NJ 08906-0971.

Please send 2 copies of all material, typewritten if possible.

Letters to the Editor, both for publication and for private reading, should be sent to the Editor at the address given above. Comments, including criticisms, are welcome, as are all suggestions for making the *Monthly* a lively, entertaining, and informative journal.

Reprint permission:
MARCIA P. SWARD, Executive Director

Advertising Correspondence:
Ms. ELAINE PEDREIRA, Advertising Manager

Subscription correspondence, change of address, and other inquiries:
Membership / Subscriptions Department

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036.

Microfilm Editions: University Microfilms International, Serial Bid coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

The AMERICAN MATHEMATICAL MONTHLY (ISSN 0002-9890) is published monthly except bimonthly June-July and August-September by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, DC 20036 and Montpelier, VT. Second class postage paid at Washington, DC, and additional mailing offices. ***Postmaster***: Send address changes to the American Mathematical Monthly, Membership / Subscription Department, MAA, 1529 Eighteenth Street, N.W., Washington, DC, 20036-1385.

The American
Mathematical Monthly

Volume 100 Number 8 / OCTOBER 1993
(ISSN 0002-9890)

Contents

ARTICLES

FEATURES

Thomas Archer Hirst—
Mathematician Xtravagant
IV. Queenwood, France and Italy

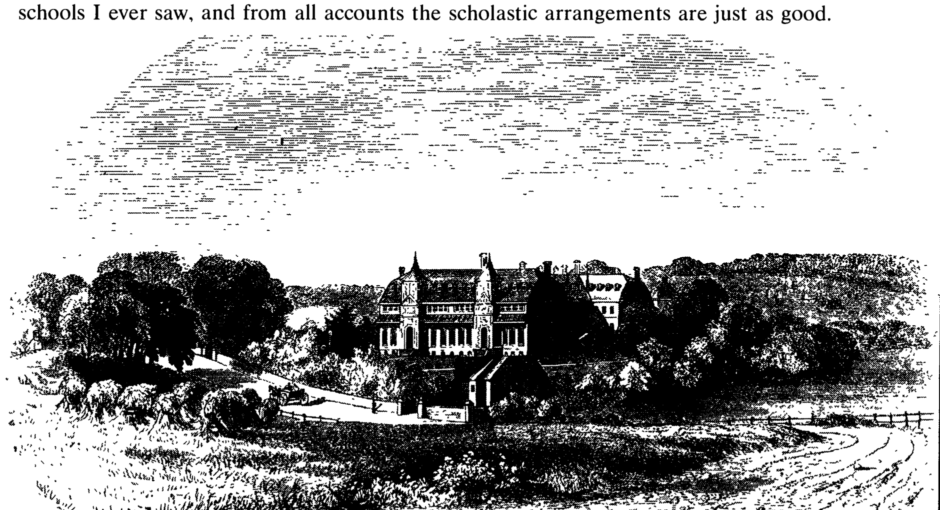
J. Helen Gardner and Robin J. Wilson

I occupied myself most of the day by sketching out a kind of inaugural lecture for Queenwood. It is now certain that in August I shall commence my life as Tutor there. It has for me its attractions and at the same time its onerous duties and responsibilities—I meet both cheerfully, and I hope for strength and courage to fulfil the task I have chosen for myself in the world.

Thomas Hirst returned to England in mid-summer 1853. At a time when there were limited job opportunities for a young mathematician, he was lucky to be offered a teaching post at Queenwood College, near Salisbury, where John Tyndall and his chemist friend Edward Frankland had taught before their Marburg days.

Queenwood College

Queenwood itself is a beautiful spot, it stands in a rich undulated chalk district, the small knowls and vallies are always graceful and smooth and the rich woods, with their beautiful beeches, yews and elms have a soothing effect. The building itself is interesting on many accounts, first, its architecture which is in a novel and picturesque style, mostly Italian. Secondly, its inward arrangements, which are the most convenient and beautiful that I have seen, and thirdly its associations, for this is the celebrated Harmony Hall, where the socialists first practically tried to live by the law of love, and of course miserably failed ... now it makes one of the most beautiful schools I ever saw, and from all accounts the scholastic arrangements are just as good.



Queènwood was partly boys' elementary school, partly mechanics' institute—a sort of technical college. There was a strong Pestolozzian influence, in that the teaching emphasized practical work by the pupils. For example, Hirst taught geometry in the context of surveying, rather than as theorems from Euclid. This experience was to prove useful later when he emerged as a reformer of geometry teaching in schools.

14th August 1853: We have now got thoroughly to work. I have 13 hours a week teaching, and two lectures; and I get more and more to love my work. The profession of schoolmaster is no drudgery, but when properly undertaken a noble task, and a healthy discipline. Yes, I have come to the conclusion that I have found my proper task, and to the determination to fulfil it to the best of my ability. At present it occupies nearly all my time, and must do until I am thoroughly master of my best plan for tuition. That done, then I sit down to my own investigations.

He was also developing a reputation for giving public lectures on physics.

30th October 1853: ... I have now conquered to a great extent all nervousness—it would be no task to speak to a thousand people about a subject with which I was well acquainted. Nevertheless, I have not yet got the tact to know what parts will be best appreciated. I found afterwards that exactly the parts on which I had laid least stress were best appreciated, and vice versa. This talent which I lack is essentially necessary to a popular lecturer...

When he could, he escaped to London to see Tyndall and to attend popular science lectures at the Royal Institution, where Tyndall was now working.

21st January 1854: Friday evening I attended Faraday's lecture—"Electricity of Induction static and dynamic effects." The lecture room was filled with a very brilliant audience, and the lecture itself pleased me much... Perhaps the lecturer's manner, person and celebrity attracted me most. There was about him such a total absence of mannerism and pretension, such geniality and gentleness...

As John and I were sitting writing, after tea this evening, Faraday himself paid us a brief visit... The room smelt villainously of tobacco, although John hurriedly scattered some eau de Cologne on the carpet. The candles too just went out and Faraday made his entrance almost in the dark. After a short time, during which Faraday had bowed to me, John remarked that I was a friend of his. "Oh, indeed!" says Faraday, fetching a chair, "well, let us all sit down, and have a look at one another." He did sit down, and after looking at me for a minute got up and shook me very kindly by the hand, saying it was a pleasure to him to know any of Tyndall's friends...

Hirst's attitude to women was somewhat prudish and patronizing. While in Marburg, he had struck up an acquaintance with a young lady called Anna Martin.

3rd July 1854: ... Instinctively I got to admire her, her artlessness, her affection for her own family, her honest independence, and even waywardness towards me, and finally her frank friendship for me in spite of all my bluntness and scolding—all these things, no doubt, besides many others, drew her nearer to me...

They were married late in 1854 at Anna's home in County Down, and returned to Queenwood after spending their honeymoon in Paris. Hirst was blissfully happy.

18th February 1855: ... I have convinced myself that she is and will be a true and devoted companion. There is in her a far deeper devotedness than I could have anticipated... I have found that her happiness consists not in comforts and luxuries, but rests on the far higher and more womanly consciousness that she is necessary to her husband's happiness... Her failings, as failings of course she has, I can trace almost entirely to her irregular life and training... yet when I *do* see her bustling about in her own cheerful, merry way I forget her inertia and consider her the best little housewife in Christendom... Let me close the passage by thanking God for her, and expressing the ever stronger determination to guard and cherish her for ever.

Married life clearly suited him, and it was also a successful time for his mathematical researches.

> **10th February 1856:** ... I have succeeded in establishing a very general and very interesting theorem with respect to the surfaces which equally attract a given point. I hope before midsummer to have a very pretty investigation ready for publication...

But it was all too good to last. Shortly after their wedding, Anna began to show signs of advancing tuberculosis. The symptoms became increasingly worse, and Hirst eventually resigned his job at Queenwood to devote himself to her. From 1856–1857 they travelled in the South of France, vainly searching for a cure. While there, he wrote two papers arising out of his earlier work at Göttingen with Gauss and Weber, and these were published in the *Philosophical Magazine*.

At the same time, his mathematical reading continued to be extensive and intelligent. Even if a work was badly written, he would persevere with it because the subject itself mattered to him. William Rowan Hamilton's work on quaternions, Carl Jacobi's *Elliptical functions* (in Latin), and Sartorius von Waltershausen's *Life of Gauss* were among the works on which he commented, often critically:

> **14th September 1856:** For the last week I have been studying Spottiswoode on Determinants in Crelle's Journal. It is obscurely written and badly printed, and hence very laborious to understand; but as I am determined to master the subject, I shall spare no pains...
>
> **18th January 1857:** ... I have purchased too an admirable work of Euler's, namely his Letters to a German Princess on subjects connected principally with Physics. The most unscientific person could understand them, they are written with wonderful clearness. I wonder a good translation of them has never been used as reading lessons in our schools. His subjects are not so elementary; it is the lucid style that deceives one into the belief that the subject is simple. Therein consists an infallible sign of an able writer...

Eventually they settled in Paris, where he made the acquaintance of a curious old fellow...

> **21st June 1857:** He is at the same time door-keeper, boot and shoe maker, and mathematician!!!! Like most self-educated men, he is extremely opinionated and almost a monomaniac. Nevertheless he is an original and altogether a remarkable shoemaker. He takes great delight in giving me problems to solve, and is disappointed when I solve them correctly. At present he pronounces my solution of the following problem to be incorrect: "A man borrows 300 francs, for which he is to pay interest at the rate of 5 per cent per ann. If he pays 20 francs a month instead of the interest which is really due, how soon will he have repaid the sum borrowed?"...

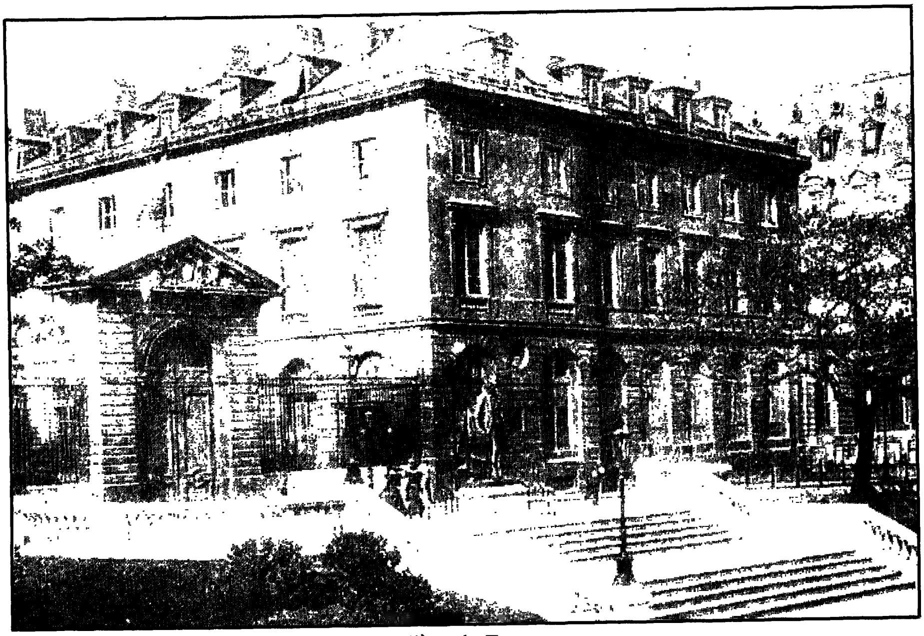
In July the inevitable happened. Anna died, leaving Hirst devastated:

> **2nd July 1857:** Poor Anna suffers no more, she is at peace for ever. Formerly she read my journal and I had always to write accordingly, to leave all my anxieties and fears unexpressed. Now she will read no more...

John Tyndall was on his way to Switzerland to study the structure and movement of glaciers, when he received intelligence of the calamity. He took Hirst with him to Switzerland, and the two became even closer friends. In August 1857 they were joined by their friend Thomas Huxley and made one of the earliest ascents of Mont Blanc.

Hirst never fully got over the tragedy of Anna's death, and paid regular visits to her Paris grave for the rest of his life. Deciding that the time had come to devote himself entirely to research, and perhaps wishing to remain near Anna, he settled himself in Paris.

18th October 1857: My health has continued on the whole good, and I have worked very steadily all the week. Still my progress does not satisfy me. When I consider that I have been nearly two months engaged on a small geometrical research which is a little out of my direct line I feel inclined to lose patience. But I must not. I have commenced a subject and I will give it some kind of finish before I pass to another...



Collège de France

As he became more involved in his researches, he resumed his practice of paying visits to mathematicians. The foremost French mathematicians at this time were Joseph Liouville and Joseph Bertrand at the Collège de France, Michel Chasles at the Sorbonne, and the retired Louis Poinsot.

18th November 1857: On Saturday last I paid M. Liouville a visit. It is long since I first entertained the idea of this visit... He is a pleasant, chatty little man with whom I soon felt at perfect ease. The only blemish I observed in him was an occasional unmeaning giggle. We talked of Dirichlet, of Steiner, of Poinsot, of Cayley and of Sylvester, in the chattiest, frankest manner. His remarks on all these men were shrewd and just. I coincided entirely. And I must confess I heard with some satisfaction his remarks on Cayley's productions. He acknowledged their ability but he protested against their wilful obscurity. He considers Cayley and Sylvester to be in some measure the disciples of Cauchy in this respect... To be precise and clear is equivalent in their eyes to being tedious. Rather than march over their difficulties and through their conquered territory with a firm, steady step, they leap and turn somersaults. It is possible that by so doing *they* are able to take a rapid and sufficient view of their subject, but others decidedly see better with their head upwards...

I went to hear Chasles' first lecture on Geometry, and was far from satisfied with it. Perhaps he was in bad humour—certainly he did not enter with his whole might into his subject. He hesitated and bungled much, and altogether his lecture formed a sad contrast to his books which are remarkably clearly written. But even his books are not to be compared to Steiner's in grasp of his subject...

Joseph Liouville (1809–1882)

Michel Chasles (1793–1880)

Much of Hirst's time was spent in translating important mathematical works into English. One such work was an important memoir on the percussion of bodies by Louis Poinsot. This gave him the opportunity to visit Poinsot at his house, where he was met by a footman and conducted to an elegant salon to meet the old man.

20th December 1857: ... He shook me kindly by the hand, bid me be seated, and took his seat near me. He is now between 60 and 70 years old, with silver silken hair neatly arranged on a fine intelligent head. He is tall and thin, but although he now stoops with age and feebleness one can see that one time his figure was more than ordinarily graceful. He was loosely but neatly dressed in a large ample robe de chambre. His features are finely moulded—indeed everything about the man betokens good blood. His eyes are now dim and dull with age, and recede far behind two prominent eyebrows. He talks incessantly and well. I did not misunderstand a word, although he spoke always in a low tone, and now and then his voice dropped as if from weariness, but he never wandered from his point...

Poinsot was delighted to discuss his works with Hirst, and was clear and interesting in his explanation of them. He seemed touched to hear of his influence on the young Hirst, remarking "We cast our seed upon the waters knowing not where it may fall, but it is nevertheless pleasant after long years of labour to find that these

seeds have taken root." He presented him with copies of all his works, which pleased the recipient greatly. Hirst obviously read them, for he was soon to write...

> **10th January 1858:** Without exception Poinsot's is the neatest and most lucid mathematical treatise I know. *I find it difficult to put down the book* just as in my younger days I found it difficult to put aside an interesting novel. Poinsot is one of the few mathematicians who dislike to leave to calculus the task and the merit of arriving at results. With most of us calculation is more than an instrument in our hands, it is a servant in our service to which servant we appoint a task and are but too prone to accept the result he brings to us without enquiring how it has been achieved—Poinsot on the contrary works *with* this servant, watches his every act and directs the same. The consequence is the result is thoroughly his own... Every thing he touches he strives to exhaust, he is not satisfied with a simple preception of a truth but he regards it from all sides laboriously and perseveringly until he has found out the path which will lead himself and others most directly and easily to the goal. For young mathematicians I should deem him an admirable instructor.

In January 1858 he received copies of a memoir he had written for Liouville's Journal, and 'saw with some little pleasure my name amongst the list of contributors on the cover', names such as Cayley, Gauss, Jacobi and Dirichlet. But this was not the only exciting event of that month...

> **17th January 1858:** On the evening of this same day the Emperor of the French [Napoleon III] narrowly escaped assassination at the entrance of the Grand Opera. As usual a crowd was assembled in the Rue Lepeletier to see the arrival of the Emperor and Empress. As their carriage drew up three loud detonations were successively heard, three infernal machines (grenades) exploded under or near his carriage killing and wounding more than a hundred of the spectators, smashing his carriage and slaying one of the horses...

His mathematical interests now took a new direction, as his work on equally attracting surfaces continually caused him to deviate into geometry.

> **31st January 1858:** ...Having found that two surfaces inscribed in the same cone attract the vertex of the latter equally, provided that radii vectors having the same direction are inversely proportional in length I am led to study what I call *inverse figures* generally. I call two figures inverse with respect to a point O chosen as the centre of inversion, when to every point A of the one corresponds a point A′ of the other so that A and A′ are on a line through O and the rectangle AO. A′O is constant...

> **14th February 1858:** ...My method of inverse transformation is leading me to a class of curves of the fourth degree which possess properties precisely analogous to but more general than conics. To every theorem in conics concerning points, lines and circles corresponds another with reference to these higher conics concerning points and circles. Conics are as it were turned inside out, their infinitely distant points becoming all concentrated in one point in the plane which I call the point of inversion.

Although he was pursuing his researches in mathematics, he maintained a strong interest in the sciences. He was particularly fascinated by the election to the membership of the Mechanical Section of the Academy of Sciences.

> **7th March 1858:** ...Foucault is a candidate. I noted last night that Chasles will not and Bertrand will support him. His not being a mathematician will in all probability be fatal. Chasles designates his gyroscope and researches on the pendulum as *happy*, but neither indicative of genius or promising in results...

Joseph Bertrand (1822–1900)

...With respect to Bertrand I am still in doubt whether his harsh, forbidding, arrogant exterior is a true index of his character or merely a cloak to a better nature. To me it is extremely disgusting, the air he assumes. His manner to me appears to repel you by the announcement "what you are telling me may interest you, but as to *me* I knew it all before and much more—in fact with respect to mathematics I am decidedly *blasé*, I may be said to have utterly exhausted that elementary science."

By April, his investigation on equally attracting surfaces was drawing to a close. Although his work had proceeded well, he was unsure of its interest or quality.

25th April 1858: ...It is strange with what different feelings I regard at different times the results of my researches. Sometimes they appear to me of tolerable interest and value, at other times merely curious and common-place. Whatever they may be I hope soon to throw them aside to the indifferent public and occupy myself with others.

6th June 1858: ...I have succeeded in integrating some partial differential equations that have caused me much trouble... I felt convinced that simple results ought to have been obtained and in fact I found after a while that a mistake where a^t was merely put in place of a had caused all the mischief. The thought of the three lost days was as nothing in comparison to the pleasure of seeing complication vanish and former results more than corroborated...

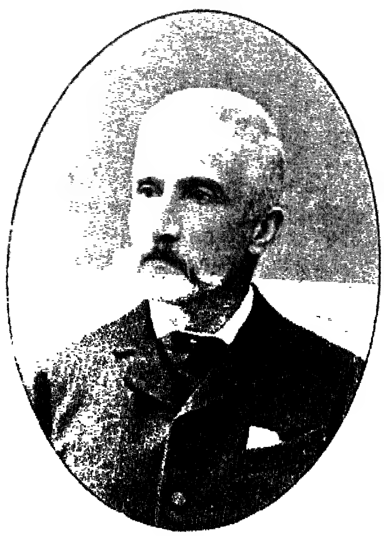
Ever since his Marburg days his health had caused him problems, which he frequently described in his diaries. In particular, toothache was a recurring problem...

13th June 1858: I have undergone the very unpleasant operation of burning the nerve. It has changed the nature of the tooth-ache, but not cured it. One night John Martin put me a leech on my gum and it bled profusely for nearly 24 hours...

Despite such problems, his work progressed well, and by the end of July he had finished his memoir on equally attracting surfaces for the *Philosophical Magazine*.

In August, he left Paris to spend almost a year in Italy—an exciting time to visit, as Italy was in the midst of Civil War.

26th April 1859: ...Austria has declared war to-day against Piedmont. On Saturday last an Austrian Aide de Camp crossed the Ticino to *invite* Sardinia to lay down her arms and disband her volunteers giving her three days to consider her reply. This news appears to be authentic. French troops are quickly moving towards the frontier, it is said they are in Genoa to-day. At any rate a fearful struggle has commenced and God knows how it will end. Its effects will be stamped upon the Century for ever...



Francesco Brioschi (1824–1897)

Luigi Cremona (1830–1903)

Most of his time was spent in Rome working with the mathematician priest Barnaba Tortolini and writing articles for Tortolini's journal. He also met mathematicians in Naples and Sicily. In June 1859 he visited the battlefields near Milan, and witnessed the aftermath of the bloody battle of Solferini.

A few days later, he received a visit from the algebraist Francesco Brioschi.

23rd June 1859: ...he is beyond doubt the ablest mathematician of Italy. He is a rather tall slightly built man with an intelligent earnest face, dark hair and beard and high good forehead, eyes of dark brown in a clear field somewhat sunk but exceedingly intelligent and penetrating... Last Autumn he visited France and Germany and made the acquaintance of the ablest mathematicians of Europe... He deems Cayley about the 1st mathematician of Europe, Hermite the first in France and Kronecker perhaps in Germany. He differed slightly as to the merits of Liouville and some others but agreed perfectly as to Bertrand, Chasles, Steiner &c... In short, of all the mathematicians I have met in Italy he produced upon me the best impression.

Even more important for the future was his first meeting with the geometer Luigi Cremona.

30th June 1859: ...He is a young man, a pupil of Brioschi's, married and has a family. He is short and has a bullet shaped bald head. Our conversation was first of all political and then mathematical; it never flagged and we parted good friends.

After two years abroad, Hirst decided that it was time to return home. After a brief visit to see friends in Marburg and visit Anna's grave in Paris, he set sail for England. The next few years in London were to be the most successful of his career, and form the topic of the next article.

ACKNOWLEDGMENTS. A typed version of the Thomas Hirst diaries is held at the Royal Institution in London, and quotations from the diaries appear here by courtesy of the Royal Institution. The diaries have been edited by W. H. Brock and R. M. MacLeod, and were published in microfiche by Mansell, London, in 1980.

Open University
Milton Keynes MK7 6AA
England

ON THE CHINESE ORIGIN OF THE SYMBOL FOR ZERO.

By Professor Florian Cajori.

I have just received a letter from Mr. Y. Mikami, of Tokyo, Japan, containing information which (if confirmed by more extended research) is of great interest and importance. The letter is dated December 15, 1902. From it I quote the following:

"I have found very important relations between the mathematics of India and of China. Arabian numerals seem to be of Chinese origin. The abacus, used by the Chinese from time immemorial, probably afforded the principle of position. In China the use of the symbol 0 for zero seems to have been very old. I desire to study the history of the Chinese mathematics from this point of view, if only I can secure sufficient materials, which is, however, very difficult. Chinese works are not [difficult] to understand for us Japanese, because we use the same letters."

Until recently the symbol for zero and the principle of local value in our notation of numbers were supposed to be of Hindu origin. A few years ago our attention was called to the early work of the Japanese, and now the priority appears to be passing to the Chinese.

COLORADO COLLEGE, COLORADO SPRINGS, *January 3, 1903.*

10(1903), 35

Thoughts on *Innumeracy*: Mathematics Versus the World?

Peter L. Renz

(A reply by John Allen Paulos follows.)

To some, mathematical calculations are soothing and reassuring. The ability to calculate gives them a sense of power. Speaking of an instance in school when his calculation was right and his teacher was wrong, John Allen Paulos wrote:

> I remember thinking of mathematics as a kind of omnipotent protector. You could prove things to people and they would have to believe you whether they liked you or not.
>
> (*Innumeracy*, page 73)

Yet his teacher did not believe Paulos's calculation and he didn't acknowledge that Paulos was correct even after seeing Paulos confirmed by figures in the *Milwaukee Journal*.

Calculation has its limits in conquering disbelief, and it has others. As basis for practical decisions or for science, calculation is limited by the accuracy of the data and the correctness of the assumptions on which it is based. Lord Kelvin calculated the age for the Earth based on the rate at which this planet cooled after its formation. He arrived at 20 million years, with 40 million years as a maximum. His calculations were correct; his assumptions were wrong. He did not know of the warming of the Earth's interior by radioactive decay. The current best estimate for the age of the Earth (again a calculation, this one based on radioactive dating) is 4.7 billion years—100 to 200 times the age that Kelvin estimated.

The relentless and immutable nature of calculation, and of mathematics in general, is an affront to some. Among the offended are the circle squarers, the angle trisectors, and the like. These people are John Allen Paulos's innumerates. Their weaknesses lead to diverse problems:

> One rarely discussed consequence of innumeracy is its link with belief in pseudoscience.
>
> (*Innumeracy*, page 4)
>
> In addition to astrology, innumerates are considerably more likely than others to believe in visitors from outer space.
>
> (*Innumeracy*, page 59)
>
> ... healthy skepticism ... a state of mind generally incompatible with innumeracy.
>
> (*Innumeracy*, page 62)

Paulos gives no quantitative evidence for these commonplace assertions. Paulos

attributes innumeracy to character faults:

> Some people personalize events excessively, resisting an external perspective, and since numbers and an impersonal view of the world are intimately related, this resistance contributes to an almost willful innumeracy.
>
> (*Innumeracy*, page 80)

But numeracy helps lift us out of the mire of personal concerns.

> If you ... see happy people holding hands, eating ice cream cones, etc., it's easy to begin to think that other people are happier, more loving, and more productive than you are, and so to become unnecessarily despondent ... It's beneficial to wonder occasionally what percentage of people you encounter suffer from this or that disease or inadequacy.
>
> (*Innumeracy*, page 81)

There is a hostile and patronizing tone here and an evident lack of sympathy for the innumerate (pity or scorn, yes; sympathy, no). These set my teeth on edge. There is an arrogance and disregard for the difficulties of others and the difficulties of applying mathematics to real problems that reflects poorly on our subject. Consistent with this, *Innumeracy* is flawed by a cavalier disregard for accuracy. Yet despite these faults, this book is a best-seller. Why?

The answer is that we already see innumeracy, however defined, as a general problem (probably in ourselves and certainly in others). Here is a book that confirms a common perception, suggests a ready cure, and does all this with amusing banter and fun number facts. Let me tempt you with this sample:

> ... take a deep breath. Assume Shakespeare's account is accurate and Julius Caesar gasped 'You too, Brutus' before breathing his last. What are the chances that you just inhaled a molecule which Caesar exhaled in his dying breath? The surprising answer is that, with probability better than 99 percent, you did just inhale such a molecule.
>
> (*Innumeracy*, page 24)

Fascinating, and for those who don't believe him Paulos gives the reader a quick calculation to prove his point. Did I believe it? No, and here is why.

Paulos states that the number of molecules in the atmosphere is about 10^{44}. Where did this number come from? I had no idea, and Paulos gives no clues, but by digging around in *The Handbook of Physics and Chemistry* I found figures for the mass of the atmosphere and the molecular constitution of the atmosphere that made his number a reasonable estimate. Next, Paulos states that a breath is $\frac{1}{30}$th of a liter and contains 2.2×10^{22} molecules. As we shall see, this is wrong on two counts. First, a gram molecular weight (mole) of any gas at standard temperature and pressure fills 22.4 liters and contains 6×10^{23} molecules. The number 6×10^{23} is Avogadro's number, the number of molecules in a mole of any compound. A quick calculation shows that Paulos should have gotten

$$\frac{1}{30} \times \frac{1}{22.4} \times 6 \times 10^{23} = 8.9 \times 10^{20}$$

molecules per breath instead of 2.2×10^{22}. But let's follow his calculation as he made it, using his number of molecules per breath. Suppose all the molecules in Caesar's last breath are uniformly mixed up in today's atmosphere. (Is this reasonable?) To get a handle on this, let's call the molecules from Caesar's last breath "lucky" and all other molecules "unlucky." The probability of a random

molecule's being lucky is just

$$\frac{\text{Number of lucky molecules}}{\text{Number of molecules in atmosphere}} = \frac{2.2 \times 10^{22}}{10^{44}} = 2.2 \times 10^{-22}$$

The probability of a random molecule's being unlucky is

$$\frac{\text{Number of unlucky molecules}}{\text{Number of molecules in atmosphere}} = \frac{10^{44} - 2.2 \times 10^{22}}{10^{44}}$$

$$= 1 - \frac{2.2 \times 10^{22}}{10^{44}}$$

$$= (1 - 2.2 \times 10^{-22}) = Q.$$

We call this number Q.

The probability of two random molecules being unlucky is effectively $Q \times Q$. (The second draw is not independent of the first because this is sampling without replacement. Calculation shows that the adjustment for dependence leaves the first twenty or so significant figures unaffected and can be neglected. Paulos makes no mention of this, although dependence can be important and the observation that it can be neglected here is a nice exercise in approximation.) The probability of your whole lungfull of molecules (all 2.2×10^{22} of them according to Paulos) consisting only of unlucky molecules is then just

$$P = Q^{2.2 \times 10^{22}} = (1 - 2.2 \times 10^{-22})^{2.2 \times 10^{22}}.$$

Paulos tells his reader that this product is less than 0.01. True, but how would an even moderately sophisticated reader calculate $(1 - 2.2 \times 10^{-22})^{2.2 \times 10^{22}}$? You can't use your pocket calculator because $1 - 2.2 \times 10^{-22}$ figured on a calculator is 1 and the exponent is out of range. Repeated multiplication is out of the question; it would take too long. You must use natural logs or the definition of e. Either approach uses calculus and yields

$$P = e^{-4.84} \approx 0.0079.$$

This is Paulos's probability of a whole lungful of unlucky molecules. So his probability of at least one lucky molecule in a random lungful is $1 - P = 1 - 0.0079 = 0.992$ or better than 99%.

What are my complaints? First, no innumerate (and relatively few numerates) could fill in the steps. Second, Paulos's numbers are wrong. If you use his $\frac{1}{30}$th of a liter per breath, the calculation gives the probability of a random breath's not containing a molecule of Caesar's last breath as

$$P' = \left(1 - \frac{8.9 \times 10^{20}}{10^{44}}\right)^{8.9 \times 10^{20}} = 0.992.$$

So the probability of getting a lungful of unlucky molecules is 0.992. (By coincidence, this number matches one in Paulos's calculation, but it gives the complementary probability.) Continuing, the probability of getting at least one lucky molecule in a lungful is $1 - 0.992 = 0.008$, or less than 1%—contrary to what Paulos writes.

What does this tell us? First, you get wrong answers from bad numbers. Second, when simple operations like addition, subtraction, multiplication, and raising to a power are taken to extremes, special techniques must be used. Third, it is not easy to dig up good values for the numbers needed in many calculations.

This calculation is mentioned without details in J. E. Littlewood's *A Mathematician's Miscellany*, and Littlewood credits James Jeans. I tracked this to Jeans's *An Introduction to the Kinetic Theory of Gasses*, Cambridge University Press, 1942. With a breath of 0.4 liter, 10^{22} molecules, this is also the number of such breaths in the atmosphere, which Jeans puts at 10^{44} molecules. With proper mixing, each breath could contain a molecule of Caesar's last breath. No fanfare. Jeans's numbers are good and his calculation is immediate. Paulos's calculation is tricky and his volume for a breath too small. The volume is close to 1/2 liter (more for a deep breath). Paulos did not check the volume of a breath either by experiment or in references. I looked at *Human Respiration* by Olof Lippold, W. H. Freeman and Company, San Francisco, 1968 and I experimented as well.

The hypothesis of random mixing of the molecules of Caesar's last breath in the atmosphere is dubious. There is no evidence that Paulos checked this. There are several problems concerning this mixing. Molecules of air dissociate and can recombine forming other molecules or react to become part of the biosphere, hydrosphere, or even end up in sediment. Looking into this requires a bit of research. Nitrogen is the main constituent of air (80% of it). The amount of nitrogen in sediment is more than that in the atmosphere. However, interchange between atmosphere and sediment is quite slow. One must check on this. My source was Delwiche's article "The Nitrogen Cycle," *Scientific American*, September 1970. These numbers are rough, but they suggest that it is safe to assume almost all the nitrogen molecules in Caesar's last breath are still in the atmosphere, but it does to speak to the uniform mixing of those molecules in the atmosphere.

We can work out Paulos's calculation with an average breath of 1/2 liter, assuming total random mixing of the original molecules of Caesar's last breath in the atmosphere, and that there is no loss of those molecules. The probability of a random breath's not containing any "lucky" molecules is

$$\left(1 - \frac{1.3 \times 10^{22}}{10^{44}}\right)^{1.3\times 10^{22}} = e^{-1.3\times 1.3} = 0.16.$$

So the probability of getting at least one lucky molecule in an average lungful is

$$1 - 0.16 = 0.84.$$

By increasing the estimated size of a breath of air you can pump this probability up to Paulos's 99%.

There is a final question here: What is the purpose of such a calculation? Is the object simply to amaze the reader, or is it to instruct, or is it intended to lead to some course of action? What do we learn from Paulos here? Jeans and Littlewood, speaking to those who could work out the technicalities, had clear points in mind, but Paulos's purpose is unclear.

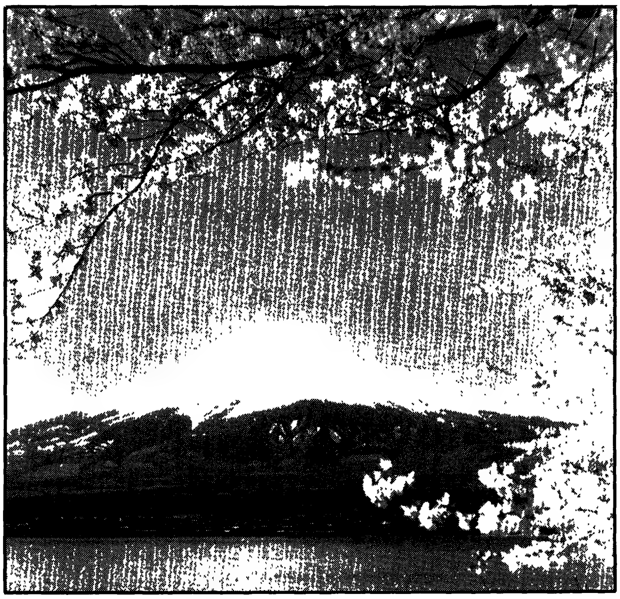
Reviewing *Innumeracy* in *The Washington Post*, Eleanor Wilson Orr, a mathematics and science teacher for 35 years and an author writing on issues in mathematics education, said, "... for the innumerate who wants to take this book seriously and read it carefully, the book is intimidating. ... I learned a lot from this book but I spent five full days reading it with a pencil in my hand. I fiddled with the numbers, I drew diagrams, I daydreamed and tried to explain to myself what Paulos doesn't explain. I trusted that I would understand it if I kept at it. Innumerates either quit or think it's enough to get the general idea, and so remain innumerate." She noted none of Paulos's errors. Judith Axler Turner, who wrote an article on Paulos and his book for the *Chronicle of Higher Education*, com-

mented that Paulos scoffed at Orr's difficulties, but I do not scoff. The last of Orr's sentences quoted in on the mark. You cannot read Paulos's book seriously without giving some attention to the details and that attention will require serious work. Not only will it require serious work but that work will reveal that there is less in Paulos's book than meets the eye of the casual reader.

Here is another numerical problem Paulos poses and answers. It is equally amusing but seems more practical.

> One last earthly calculation that a scientific consultant from M.I.T. uses to weed out prospective employees during job interviews: How long, he asks, would it take dump trucks to cart away an isolated mountain, say Japan's Mount Fuji, to ground level? Assume trucks come every fifteen minutes, twenty-four hours a day, are instantaneously filled with mountain dirt and rock, and leave without getting in each other's way. The answer is a little surprising and will be given later.
> (*Innumeracy*, page 12)

The answer, without explanation, appears in a sentence on page 15 where Paulos estimates it would take 5,000 to 10,000 years to truck away Mount Fuji. This is a surprisingly short time for such a job. It is also wrong. The only fact that Paulos mentions about Mount Fuji is its height, 12,000 feet, so it is clear that he figured the mountain was some sort of cone. The volume of a cone is a third of its base area multiplied by its height, a fact easily derived and known to Archimedes. Evidently, Paulos must have also used the area of the base of Mount Fuji in his calculation. Did he look this up? Did he consult maps? No, as an exchange of letters revealed, he dreamed it up. He assumed Mount Fuji was a cone as wide at its base as it was high. Volcanos are simply not shaped this way, and one might expect Paulos, who spent a year at the University of Washington within easy view of Mount Rainier, to know something about the shape of a volcano. Leaving that aside, you might expect him, as an author, to look at an atlas. I did. The map is revealing. It shows that Fuji is roughly conical and has a radius of about 12 kilometers at its 1000 meter contour. Its height is 3776 meters above sea level. Below 1000 meters it broadens out considerably. We might construe the problem of trucking away Mount Fuji as that of taking enough of it away so that what was left would blend into the countryside. From the map it looks as if taking the top 2776 meters off the peak would do the job. The volume of that part of the



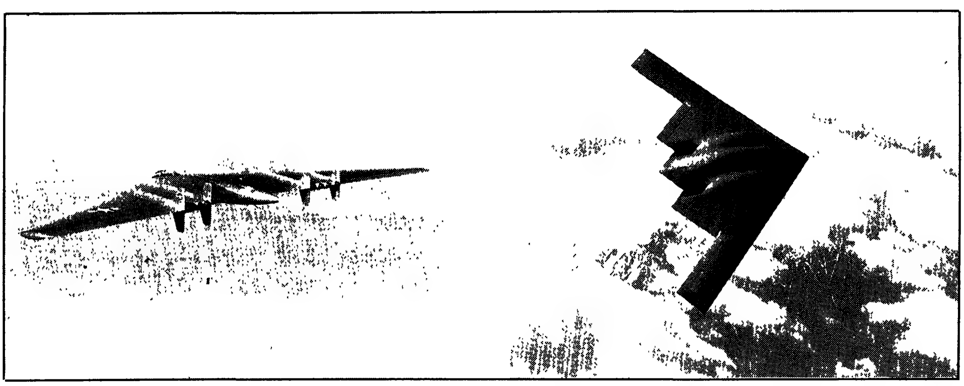
The gentle slopes of Mount Fuji are shown here. Photograph courtesy of the Japan National Tourist Organization.

mountain is

$$\tfrac{1}{3} \times \pi(12{,}000\ m)^2 \times 2776\ m = 4.19 \times 10^{11}\ m^3.$$

Calling a local importer of heavy Japanese trucks, I found that the largest standard model that they imported could carry 18.5 cubic yards. Round up to 20 cubic meters per load, and divide by the product—cubic meters per load times loads per hour times hours per day, etc.—and you will find that it would take about 600,000 years to truck away the top 2776 meters of Mount Fuji, To cart away a cone the same shape and the height of Mount Fuji measured from sea level (3776 meters) would take over 1.5 million years at this rate. Paulos's estimate of 5,000 to 10,000 years is off by orders of magnitude. Would his mythical M.I.T.-based recruiter have hired him for some practical job? I would hope not, but given the errors committed in real-world engineering, perhaps so. Note that even with these considerations, this is a highly idealized problem. It is clear that no such project could ever be carried out.

Here is an example of real-life erroneous calculation with a potentially large impact. These calculations were made by William R. Sears and Irving L. Ashkenas in a secret assessment of promising aeronautical technologies that they prepared in 1945. Sears and Ashkenas built a mathematical model to show how the range of an aircraft varied as one redistributed the volume between the wing and the fuselage. Sears and Ashkenas were working at the time for the Northrop Corporation, a firm then building various experimental "flying wing" aircraft. They differentiated their formula for range as a function of the percentage of volume in the wings and found only two possible extrema: one of these was when all the volume was in the wing and the other when a much smaller fraction of the volume was in the wing. Sears and Ashkenas wrote, "It can be ascertained that the form [all volume in the wing] gives maximum range, while the latter gives a minimum." Hence, flying wings have the maximal range.



The Northrop YB-49 Flying Wing, left, and its sleek delta-form descendant, the B-2 Stealth bomber, right. Both pictures courtesy of the Northrop Corporation.

Joseph Foa, who headed a group studying possible designs for an unmanned jet aircraft at Cornell Aeronautical Laboratory (CAL) had reached the contrary conclusion—that a flying wing configuration would not give maximum range. After Sears came to head CAL, Foa had a chance to examine the Sears-Ashkenas report and discovered that the critical point associated with the flying wing configuration

was a minimum, not a maximum. It gave the minimum range according to their model, not the maximum range, as Sears and Ashkenas claimed.

This came to light in *Science* (Volume 244, pp. 650–651, 12 May 1989) in connection with controversy about the B-2 stealth bomber, also a flying wing. In the 1940s Foa kept his silence on the condition that Sears and Ashkenas publish some sort of correction to their earlier analysis. That correction took the form of the 1948 paper "Range performance of turbojet airplanes" by Ashkenas in the *Journal of the Aeronautical Sciences*. Here Ashkenas made a much more complex mathematical model, which had the property that the flying wing configuration gave optimal range for certain choices of the basic parameters. To this day Foa remains unconvinced, asserting that the Ashkenas optimum flying wing would be impractically thick.

The B-2 project had a multi-billion dollar budget. The initial error of Sears and Ashkenas, mistaking a minimum for a maximum, is a classic for students in freshman calculus. But even after careful consideration by competent aeronautical engineers, it is not clear whether the flying wing is the best or the worst way to go if one wants a long-range plane. The answer you get from a mathematical model seems to depend on what answer you want to get.

Our quantitative understanding of the world is not simply based on assumptions; it is based on observation. Generally there is a lot of hard work needed to get good numbers. When it comes to projecting cancers that may or may not be caused by the breakdown products of minute quantities of Alar in apples, the work is hard, the numbers are soft, and the theoretical apparatus is quite involved. The meaning of such calculations is more controversial, important, and uncertain than for the calculations I have discussed above. Paulos gives scant attention to any of this.

Paulos is quick to point out the problems of others.

> A recent study by Drs. Kronlund and Phillips of the University of Washington showed that doctors' assessments of the risks of various operations, procedures, and medications (even in their own specialities) were way off the mark, often by several orders of magnitude.
>
> (*Innumeracy*, page 8.)

Paulos continues in the cited paragraph, heaping scorn on doctors, "I once had a conversation with a doctor who, within approximately twenty minutes, stated that a certain procedure he was contemplating (a) had a one-chance-in-a-million risk associated with it; (b) was 99% safe; and (c) usually went quite well. Given the fact that so many doctors seem to believe that there must be at least eleven people in the waiting room if they're to avoid being idle, I am not surprised at this new evidence of their innumeracy." Let's think this through. If (a) is true, then (b) follows, because it is a weaker condition. Furthermore, it is reasonable (c) might also be true. A doctor might say that such a procedure "usually went well," although this is a qualitative judgment having to do with ease of the procedure and lack of difficulties for the doctor. Now, I expect the doctor in question did not have much detailed statistical information, because such information is difficult and costly to gather. But does what Paulos present show the doctor to be innumerate? Not at all, and the line about waiting rooms is a cheap shot meant to please readers who have cooled their heels in a doctor's office.

The importance and the difficulty of gathering good data on medical matters are greater than one might think. Let me use an example from *Innumeracy*. Paulos begins a calculation on page 21 by stating that the probability of heterosexual

transmission of AIDS from an infected to an uninfected person is 0.002 per act of intercourse. This probability is called the infectivity. He says this is an average of figures from several studies—but he cites no sources. This makes me wonder, because it is difficult to see how one could get good figures on the transmissibility of this disease. Only a Dr. Mengele operating without restraint could plan and execute experiments on AIDS infectivity. The problems include the facts that AIDS is sexually transmitted and 100% fatal. It is extremely difficult to get accurate information about sexual behavior. These matters are private and sensitive. People regularly lie about sexual matters, and Congress regularly kills publicly-funded studies of sexual behavior.

I asked experts, including Eric Lander who organized the National Academy of Sciences session on AIDS, about reliable information on the heterosexual transmissibility of AIDS and came up with little. The best source I found was the issue of *Los Alamos Science*, Number 18, 1989, devoted to AIDS. The lead article, "AIDS and a Risk-Based Model," by Colgate, Stanley, Hyman, Qualls, and Layne, gives estimates for the infectivity ranging from 0.0014 to 0.004 . These authors cite others whose estimates of the infectivity run from 0.003 to 0.1. The methods discussed are difficult and use epidemiological data and complex assumptions. There is a factor of about 100 between the largest and smallest of these estimates of infectivity, and Paulos's 0.002 falls within the range, on the low side. It would be prudent not to put too much faith in any particular number for the infectivity.

Let's see what use Paulos makes of this probability. He says we may assume these probabilities of transmission to be independent. He then notes that $(1 - 0.002)^{346} \approx 0.5$. So that a year's worth of nightly unprotected intercourse with an infected partner leaves you with a better than 50% of being uninfected. Next, he asserts that if a condom is used the infectivity drops to 2×10^{-4}. Now you can enjoy ten years of nightly intercourse with the victim (assuming the victim lives this long, Paulos adds parenthetically) before your probability of getting AIDS rises to 0.5. Finally, Paulos states that the probability of contracting AIDS from a single act of unprotected intercourse with someone belonging to no known risk group is 2×10^{-7} and with a condom this probability drops to 2×10^{-8}. He writes that you will more likely die in a car accident returning from such a tryst than catch AIDS during the act. All this suggests that one need not worry all that much about AIDS. Now these calculations are correct, though the assumptions underlying them are dubious, and the suggestion that AIDS is not very worrisome is dead wrong.

AIDS transmission is extremely variable. It appears that an individual can be so infectious as to infect virtually everyone with whom he has unprotected sexual intercourse. The evidence for this comes from an Australian sperm donor. His frozen sperm sample was split into ten doses, eight of which were used, resulting in four infected women. A Poisson model is suggested for assaying infectivity by dilution methods in "The Kinetics of HIV Infectivity," by Layne, Dembo, and Spouge in the cited issue of *Los Alamos Science*. Let N be the number of individuals treated with the diluted infectious agent (here, $N = 8$). Let d be the dilution that infects 50% of the individuals treated (here $d = 0.1$), and I be the infectivity of the undiluted semen. Then in this instance

$$\text{Number infected} = 4 = 0.5N = Ne^{-dI} = Ne^{-0.1I}.$$

The exponential factor comes from the Poisson probability,

$$p_k = e^{-dI}(dI)^k/k!$$

with $k = 0$. Using this we can estimate the probability of infection from a single act of intercourse with this donor at the time of donation

$$1 - \text{Probability of no infection} = 1 - e^{-I} = 1 - \frac{1}{2^{10}} \approx 0.999$$

where the probability of no infection is simply obtained from the Poisson p_0 with $d = 1$ and I evaluated from $0.5 = e^{-dI}$.

Not much data is available. But to illustrate the variability of transmission of AIDS, I quote another example. Sperm from an infected New York donor was used to inseminate 90 women, none of whom contracted AIDS. Even given selectivity in reporting, it is unlikely that the cited Australian and New York examples are samples drawn from the same population.

What of Paulos's comment about the risk of being killed in an automobile accident versus the risk of getting AIDS? It is a common and generally uncalculated guess that the risks of doing X are less than the risk of driving to the place where you do X. From Paulos's figures, it might be the other way around in this case. The average US passenger death rate as given in *The World Almanac and Book of Facts*: 1992 is 1.12×10^{-8} deaths per mile. Compare to Paulos's estimate of a risk of 2×10^{-8} for contracting AIDS from protected intercourse with someone having no known risk factors. The risk that dominates will depend, at least, on how far away the tryst is. More importantly, the death rate per mile depends strongly on the age, sex, and driving history of the driver and on such things as sobriety, roads and road conditions, and on whether a seat belt is used. Your risk per mile could be quite a bit larger or smaller than the average which I gave. As we begin to bring in these considerations, we move from a general statistical treatment toward special cases and special pleading. More data would be needed to establish the risks for these new classes. This leads away from easy calculation and toward more specialized cases. This sort of thinking is a poor guide for public policy, but we live or die as special cases, not on the average.

This simply hints at what is wrong with the lax, breezy treatment Paulos gives. When applied to so serious a matter as AIDS, it is shocking. Yes, innumeracy is a problem, but *Innumeracy* is more a part of the problem than of the solution. This need not have been the case. Were the book less negative toward the innumerate and more carefully done, it could have made a wonderful contribution. My copy has quite a few favorable comments in the margins along with many notes on errors of the sort I mentioned here.

We should hold ourselves, our students, and others to higher standards. We want public appeal, clarity, and *truth*. This will not be easy to get, but why settle for less?

101 Colchester Street
Brookline, MA 02146

John Allen Paulos replies:

A distant relative of mine recently returned from a three-month stay in Florida. When I asked him how it was, he launched into a detailed disquisition on the mechanical minutiae of his new appliance for extracting juice from oranges and grapefruits. He took offense at my attempt to summarize his comments or to use

Reflections on Rippling Water

Michel Mendes France

1. INTRODUCTION. On a summer evening standing beside a large lake that extends to the horizon, we observe the moon's reflection on the rippled surface of the water. When the moon is low, but nonetheless completely above the horizon, the reflection may still appear as a long uninterrupted yellow column which stretches from some point on the lake to the horizon. Its length can be considered as infinite. Later, when the moon rises higher up in the sky the reflection changes aspect and becomes a shorter beam, in the shape of a narrow oval. It is closer to us and no longer extends to the horizon. Its length is now finite.

Stars may appear in this evening sky. If a gentle breeze is blowing, each one of these stars will appear to be reflected an odd number of times in a given direction on the surface of the lake.

These evocative images raise interesting mathematical questions. At what angle does the moon's reflection change from an infinite image to a finite one? Is it possible to see exactly two reflections of the same star? The object of this paper is to answer these questions. Our analysis only requires simple trigonometry.

2. THE THEORY. Suppose an observer at height H_1 sees a reflected object on the wavelet M at a distance x across the water.

Let $\alpha = \alpha(x)$ be the angle measured in radians between the normal MN to the wave with the vertical V. Let α_0 be the maximal value of $|\alpha(x)|$ and define $\varphi(x)$ by $\alpha(x) = \alpha_0\varphi(x)$ so that $|\varphi(x)| \leq 1$. Let i be the angle of reflection (Figure 1 and 2).

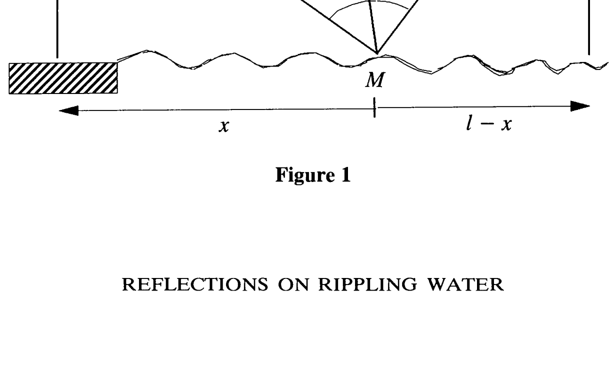


Figure 1

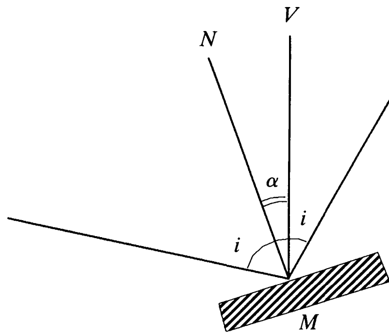


Figure 2

Trivial trigonometry shows that

$$\begin{cases} \tan(i+\alpha) = \dfrac{x}{H_1} \\ \tan(i-\alpha) = \dfrac{l-x}{H_2}. \end{cases}$$

Hence

$$\begin{aligned} \tan 2\alpha &= \tan[(\alpha+i)-(i-\alpha)] \\ &= \frac{\tan(\alpha+i)-\tan(i-\alpha)}{1+\tan(\alpha+i)\tan(i-\alpha)} \\ &= \frac{\dfrac{x}{H_1}+\dfrac{x-l}{H_2}}{1+\dfrac{x(l-x)}{H_1H_2}} = \frac{(H_1+H_2)x-lH_1}{H_1H_2+lx-x^2}. \end{aligned}$$

We now assume that α_0 is small. Then

$$2\alpha \approx \frac{(H_1+H_2)x-lH_1}{H_1H_2+lx-x^2}.$$

Finally,

$$\varphi(x) \approx \frac{(H_1+H_2)x-lH_1}{2\alpha_0(H_1H_2+lx-x^2)}. \tag{1}$$

Before exploiting the relationship given by (1), let us analyze the corresponding equation

$$\varphi(x) = \frac{x(H_1+H_2)-lH_1}{2\alpha_0(H_1H_2+lx-x^2)}. \tag{2}$$

Note that each side of (2) has a physical interpretation. The function φ describes the shape of the waves while the right-hand side represents the distance at which a reflection occurs. So, for a given shape φ, the solutions of (2) are the approximate distances at which a reflection occurs. In particular, the number of solutions is the number of reflected images we see.

Now let us analyze the equation. We start by looking at the simplest case when there are no waves at all: $\varphi \equiv 0$. Then

$$x = \frac{lH_1}{H_1 + H_2}.$$

Thus there is only one reflection so that the observer sees a perfect image of the object. If, in particular $H_1 = H_2$, then $x = l/2$ and the light ray is reflected at the midpoint between the observer and the object. This is of course well known.

Let us now discuss the general case where φ stays small. We solve the equation (2) graphically.

Let β be the curve

$$\beta\colon x \mapsto \frac{x(H_1 + H_2) - lH_1}{2\alpha_0\left(H_1H_2 + lx - x^2\right)}.$$

In the interval $(0, l)$, β is continuous and increasing. Furthermore

$$\beta(0) = -\frac{l}{2\alpha_0 H_2} \quad \text{and} \quad \beta(l) = \frac{l}{2\alpha_0 H_1}.$$

We assume that both H_1 and H_2 are strictly less than $l/2\alpha_0$ (l is large and α_0 is small).

The curve $x \mapsto \varphi(x)$ oscillates in the horizontal strip $y = -1$, $y = +1$. Supposing φ is continuous in the interval $[0, l]$, both curves intersect either at an odd number of points or infinitely often. Thus, whatever the shape of the waves may be, one should see either an odd number of reflections, or infinitely many. (This last case may indeed occur if, for example, φ has a singularity of the type $(x - a)\sin(x - a)^{-1}$ in the neighbourhood of some $a \in (0, l)$).

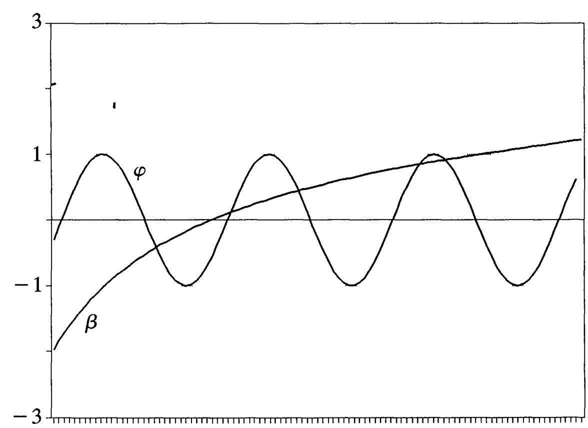


Figure 3

3. LIMITING CASES. Let us study the solutions of equation (2) when $l = +\infty$ (reflection of the moon or the sun...).

We denote by w the angle at which the infinitely far away object is seen. Then H_1/l is negligible and $H_2/l = \tan w$. Thus rewriting the right hand side of equation (1) in the form

$$\frac{x\left(H_1 l^{-1} + H_2 l^{-1}\right) - H_1}{2\alpha_0\left(-\dfrac{x^2}{l} + x + \dfrac{H_1 H_2}{l}\right)}$$

we have

$$\varphi(x) \approx \frac{x \tan w - H_1}{2\alpha_0(x + H_1 \tan \omega)} = \gamma(x).$$

As before we solve the equation $\varphi(x) = \gamma(x)$ graphically and we suppose that φ oscillates a great many times, say

$$\varphi(x) = \sin \lambda x$$

where λ is large. We solve equation (3) for $x \in (0, l)$

$$\sin \lambda x = \gamma(x). \tag{3}$$

Since $\gamma(x)$ is monotonically increasing we know that the smallest solution x_S of (3) occurs when this function is -1 and the largest solution x_L occurs when the function is $+1$.

When $\tan w < 2\alpha_0$, we see from Figure 4 that the two curves intersect infinitely many times and the smallest solution is approximately

$$x_S \approx \max\left\{0, H_1 \frac{1 - 2\alpha_0 \tan w}{\tan w + 2\alpha_0}\right\}.$$

In this case, the reflection on the water extends from x_S to the horizon. When $\tan w > 2\alpha_0$, the solution is shown on Figure 5.

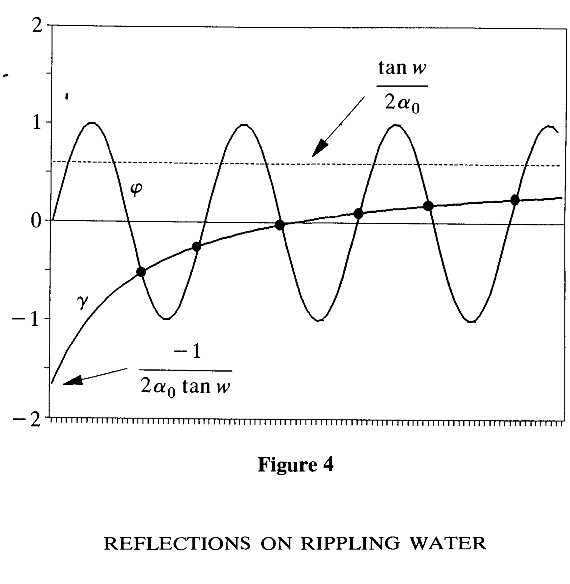


Figure 4

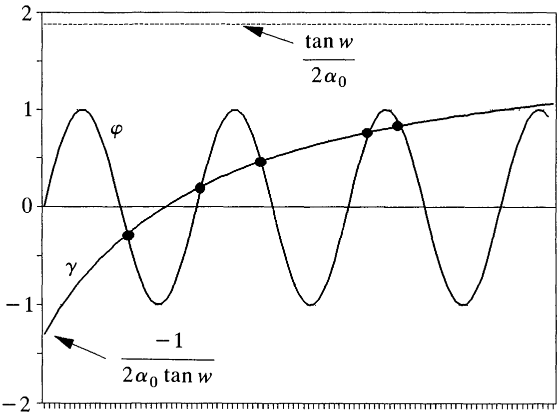


Figure 5

In this case there is only a finite odd number of reflections and the reflections lie between x_S and x_L

$$x_L \approx \frac{H_1}{\tan w - 2\alpha_0}(1 + 2\alpha_0 \tan w).$$

It follows that the critical w_c at which the reflection ceases to be infinite is therefore

$$w_c = \tan^{-1}(2\alpha_0).$$

As α_0 is assumed to be small, we have

$$w_c \approx 2\alpha_0.$$

Finally, if one is given the shape of the waves as a Cartesian equation

$$y = \psi(x),$$

then

$$\alpha(x) = \tan^{-1}\psi'(x),$$

provided ψ is differentiable. As $|\alpha(x)|$ is small, this entails $\alpha(x) \simeq \psi'(x)$ so that the critical angle is

$$w_c \approx 2\max_x |\psi'(x)|.$$

4. AN APPLICATION. The amplitudes of real waves on the ocean, far away from the coast (say 100 yards or more) are difficult to measure: they move rapidly and their size may be small, especially if we are discussing wavelets or even ripples. On the other hand, w_c can be quite easily measured at sunset: observe at what angle w_c the reflection starts to touch the horizon. If we assume that during that time of waiting, the waves keep approximately the same shape, say

$$\varphi(x) = \alpha_0 \sin \lambda x \cos \lambda ct$$

where c is the velocity of the wave and t is time, then the knowledge of w_c and of the frequency λ gives us the amplitude A of the waves

$$A = \frac{w_c}{2\lambda}.$$

Our analysis is also valid for studying the microscopic structure of a glossy surface. The macroscopic observation of a reflecting luminous point provides information on the fine structure of the surface. Determining w_c measures the product $A\lambda$.

It was only after completing this work that I discovered M. Minnaert's delightful book [1] on the "Nature of Light & Colour in the open air." It discusses related topics and I highly recommend it (see in particular pp. 23–26). I wish to thank the referee and Jacques Harthong for helping me to improve the exposition and the graphs.

Addendum. Many authors have studied the reflection on rippling water. I would like to single out M. V. Berry's beautiful article "Disruption of images: the caustic-touching theorem," *J. Opt. Soc. Am. A.* 4, 1987, pp. 561–569.

REFERENCE

1. M. Minnaert, *The Nature of Light & Colour in the Open Air*, Dover Publ., Inc., 1954.

Department of Mathematics
Université Bordeaux I
F-33405 Talence Cedex
France

PICTURE PUZZLE
(from the collection of Paul Halmos)

Are they related?
(see page 809.)

The Principal Axis Theorem over Arbitrary Fields

David Mornhinweg, Daniel B. Shapiro, and K. G. Valente

The Principal Axis Theorem, included in most undergraduate texts in Linear Algebra though often without proof, states that every symmetric matrix over the field of real numbers is orthogonally similar to a diagonal matrix. In **[1]**, S. Friedberg, focusing attention on the underlying field, gave an elementary argument to show that there are symmetric matrices over $\mathbf{Z}_p$ (p a prime) which are not orthogonally similar to a diagonal matrix. This paper concludes with a problem: "Classify exactly those fields for which the Principal Axis Theorem is true." As solutions to this classification problem can be found in the literature (see **[2]** and **[10]** for example) and frequent reconsiderations of this topic indicate an interest to a wide audience of mathematicians, the purpose of this paper is to give a simplified overview of this beautiful result. As we proceed, we keep an eye toward the accessibility of the argument. In fact, with the exception of two technical results, this development can be incorporated in any undergraduate-level course in Linear Algebra that deals with arbitrary fields. For example, one can show quite easily that it is necessary for the field to have characteristic equal to zero in order to insure that symmetric matrices are diagonalizable. While it is a rather straightforward matter to establish a large class of fields which allows for the orthogonal diagonalization of symmetric matrices, one of the aforementioned technical results is crucial in the final step of the classification of such fields.

A field F is said to have the *Principal Axis Property* if every symmetric matrix over F is orthogonally similar to a diagonal matrix over F. That is, for every symmetric matrix M over F, there exists an orthogonal matrix P over F (that is, $P^{-1} = P^t$) such that $P^{-1}MP$ is diagonal.

A study of the 2×2 case provides some important information. We write char(F) for the characteristic of F.

Lemma 1. *Suppose every symmetric 2×2 matrix over F is diagonalizable over F. Then*

(i) $\sqrt{-1} \notin F$,
(ii) *every sum of squares in F is a square in F, and*
(iii) char$(F) = 0$.

Proof: Just suppose there exists $i \in F$ with $i^2 = -1$. Then the matrix

$$\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}$$

has characteristic polynomial x^2. If this matrix were diagonalizable, it would have to be the zero matrix. This contradiction establishes (i). As an immediate consequence we have char$(F) \neq 2$, for if char$(F) = 2$, then $i = 1 = -1$ in F.

To prove (ii) it suffices to show that if $a, b \in F$ then $a^2 + b^2$ is a perfect square in F. To see this we consider the matrix

$$M = \begin{bmatrix} a & b/2 \\ b/2 & 0 \end{bmatrix}$$

which has eigenvalues $\frac{1}{2}(a \pm \sqrt{a^2 + b^2})$. Since M is diagonalizable over F, we know that these eigenvalues lie in F, so that $\sqrt{a^2 + b^2} \in F$. Property (iii) now follows from (i) and (ii), for if $\mathrm{char}(F) = p > 0$ then $-1 = (p - 1)$ is a sum of squares in F. $\square$

Every field satisfying the conditions of Lemma 1 must possess an "ordering". To explain why this is so, we outline some of the properties of ordered fields. These ideas were introduced by E. Artin and O. Schreier in the 1920's and have since appeared in many algebra texts. The basic idea is that an order relation on F, which respects the field operations of F, is determined by the "cone" P of non-negative elements. This P is taken as the fundamental object.

Definition. An *ordering* on a field F is a subset $P \subseteq F$ satisfying (i) $P + P \subseteq P$; (ii) $P \cdot P \subseteq P$; (iii) $P \cap -P = \{0\}$; (iv) $P \cup -P = F$.

Here $-P := \{-a : a \in P\}$. Given an ordering P, we define an order relation $\leq$ on F as follows: $a \leq b$ if and only if $b - a \in P$. The reader is invited to derive the familiar properties of "less-than-or-equal" from the given axioms. For example, $a^2 \geq 0$ for every element a. This follows from (ii) if $a \in P$. Otherwise, $a \notin P$ and (iv) implies that $-a \in P$, so that $a^2 = (-a)^2 \in P$. From (i) it follows that every sum of squares in F must lie in P. This proves that if F admits an ordering, then F must be "formally real" in the following sense.

Definition. A field F is *formally real* if -1 is not expressible as a sum of squares in F.

From our remarks above, we see that the complex field $\mathbb{C}$ has no ordering. Also if $\mathrm{char}(F) > 0$, then F has no ordering. However some fields admit several orderings. For instance if $\sigma : F \to \mathbb{R}$ is a homomorphism into the field of real numbers, then $P = \sigma^{-1}([0, \infty))$ is an ordering on F. Distinct embeddings of F into $\mathbb{R}$ yield distinct orderings of F. For example $\mathbb{Q}(\sqrt{2})$ possesses two orderings.

Our first technical result completes the connection between ordered and formally real fields.

Theorem 1. *A field F admits an ordering if and only if F is formally real.*

This famous theorem was first proved by Artin in the 1920's as part of his solution to Hilbert's 17th problem. The construction of an ordering on a formally real field invokes the Axiom of Choice and appears in a number of texts, including [7], [**8**] and [**9**].

The second property appearing in Lemma 1 has also been given a name.

Definition. A field F is *pythagorean* if every sum of squares in F is a square in F.

The fields of real and complex numbers are pythagorean, while the field of rationals is not. Using this new terminology, Lemma 1 can be restated as follows: if 2×2 matrices over F can be diagonalized over F, then F must be formally real and pythagorean. Therefore, in our search for fields which satisfy the Principal Axis Property, we may restrict our attention to formally real pythagorean fields. We now point out that such fields allow for the Gram-Schmidt orthogonalization process on F^n.

Lemma 2. *Let F be a formally real pythagorean field and let $\geqslant$ be any order relation on F. If $\mathbf{u} = (u_1, \dots, u_n)$ and $\mathbf{v} = (v_1, \dots, v_n)$ in F^n, define*

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 + \cdots + u_n v_n .$$

Then this map $\langle \cdot , \cdot \rangle$: $F^n \times F^n \to F$ is an inner product, and for every $\mathbf{v} \in F^n$ there exists a unique element $\|\mathbf{v}\| \in F$ with $\|\mathbf{v}\| \geqslant 0$ and $\|\mathbf{v}\|^2 = \langle \mathbf{v}, \mathbf{v} \rangle$.

Proof: For $\mathbf{v} \in F^n$ we see that $\langle \mathbf{v}, \mathbf{v} \rangle = v_1^2 + \cdots + v_n^2 \geqslant 0$ in F. Moreover if $\mathbf{v} \neq \mathbf{0}$ then some $v_i \neq 0$ and $\langle \mathbf{v}, \mathbf{v} \rangle \neq \mathbf{0}$. It follows that $\langle \cdot , \cdot \rangle$ is an inner product. Since F is pythagorean we know that $\langle \mathbf{v}, \mathbf{v} \rangle$ is a square in F. Every square in F has a unique non-negative square root in F, and the lemma follows. □

We are now in a position to rephrase the question found in **[5]**.

Theorem 2. *Let F be a formally real pythagorean field. The following are equivalent:*

(i) *F has the Principal Axis Property,*
(ii) *Every symmetric matrix over F is diagonalizable over F, and*
(iii) *Every symmetric matrix over F has an eigenvalue in F.*

Proof: Clearly (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). To prove (iii) $\Rightarrow$ (i) we let M be an $n \times n$ symmetric matrix over F and proceed by induction on n. The result is clear when $n = 1$ so we may assume $n > 1$. Let $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be the standard orthonormal basis of F^n. By (iii) the matrix M has an eigenvalue $k \in F$, and there exists a corresponding eigenvector $\mathbf{w} \in F^n$. Complete this vector to a basis of F^n, and apply the Gram-Schmidt process to obtain an orthonormal basis $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$, where $\mathbf{u}_1 = \mathbf{w}/\|\mathbf{w}\|$. Let P be the matrix with columns equal to these vectors $\mathbf{u}_i$ and let $S = P^{-1}MP$. Then P is an orthogonal matrix since the columns form an orthonormal basis. Therefore S is also symmetric. The first column S is $S\mathbf{e}_1 = P^{-1}MP\mathbf{e}_1 = P^{-1}M\mathbf{u}_1 = k \cdot P^{-1}\mathbf{u}_1 = k\mathbf{e}_1$. The first row of S is then determined by the symmetry and we see that

$$S = \begin{pmatrix} k & 0 & 0 & \cdots & 0 & 0 \\ 0 & & & & & \\ 0 & & & & & \\ \vdots & & & S_0 & & \\ 0 & & & & & \\ 0 & & & & & \end{pmatrix}$$

where S_0 is a symmetric $(n-1) \times (n-1)$ matrix. By induction, there exists an $(n-1) \times (n-1)$ matrix R_0 such that $R_0^{-1} = R_0^t$ and $R_0^{-1}TR_0 = D$ where D is a

diagonal matrix. Now, set

$$R = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & & & & & \\ 0 & & & & & \\ \vdots & & & R_0 & & \\ 0 & & & & & \\ 0 & & & & & \end{pmatrix}$$

and consider the matrix PR. We see that $(PR)^{-1} = (PR)^t$, and

$$(PR)^{-1}M(PR) = \begin{pmatrix} k & 0 & 0 & \cdots & 0 & 0 \\ 0 & & & & & \\ 0 & & & & & \\ \vdots & & & D & & \\ 0 & & & & & \\ 0 & & & & & \end{pmatrix}. \quad \square$$

We note that when working over the field of reals or real algebraic numbers one can appeal to the standard arguments involving the Fundamental Theorem of Algebra to conclude by Theorem 2 that all symmetrics can be diagonalized. In particular, both of these fields are real closed. For our purposes, a field F is *real closed* if it is pythagorean, formally real, and $F(\sqrt{-1})$ is algebraically closed. (There are many other equivalent definitions for real closed.) This class of fields was also studied by Artin and Schreier and further information regarding these fields can be found in the aforementioned texts.

This theorem also implies that an intersection of fields satisfying the Principal Axis Property again has that property, although some care must be taken to ensure that the intersection makes sense. To guarantee that the field operations are compatible, we assume that all the fields in question are subfields of some larger field.

Corollary.

(i) *Any real closed field satisfies the Principal Axis Property.*

(ii) *Let Ω be a field with $\{F_\alpha\}$ a collection of subfields. If each field F_α satisfies the Principal Axis Property, then their intersection also satisfies the Principal Axis Property.*

Proof: Using the definition of real closed given above, the standard argument establishing the existence of a real eigenvalue for a real symmetrix matrix can be adapted to prove (i). For a more complete development of diagonalization over real closed fields, one can also see [**9**].

To prove (ii) let $F = \bigcap_\alpha F_\alpha$ be the intersection. By Lemma 1 and the subsequent definitions, we know that each F_α is formally real and pythagorean, and therefore so is F. If M is a symmetric matrix over F, then Theorem 2 implies that all of the eigenvalues of M lie in F_α. Since this is true for every α, we see that the eigenvalues lie in F. The claim follows by another application of Theorem 2. $\square$

With this corollary we see that the intersection of any collection of real closed fields (that are subfields of a common field) satisfies the Principal Axis Property.

In fact, these are only fields with this property. To see this we are in need of a second technical result due to F. Krakowski [**6**]. As before, we must assume all the fields under consideration lie inside some larger field. To this end, let F be a field with Ω a fixed algebraically closed extension of F. Set

$$R(F) = \bigcap \{K | F \subseteq K \subseteq \Omega \text{ and } K \text{ is real closed}\}.$$

Note, using Theorem 1, if F is not formally real, then $R(F)$ is trivial. On the other hand, if F is formally real, then $R(F)$ is a formally real pythagorean extension of F. Further information regarding the construction of $R(F)$ can be found in [**3**], [**7**] and [**10**].

Theorem 3. *Let F be a formally real pythagorean field. For any $a \in R(F)$, there exists a symmetric matrix over F having a as an eigenvalue.*

Proof: (Sketch) Let V denote the field $F(a)$ with $B: V \times V \to F$ the trace form. That is,

$$B(x, y) = \mathrm{tr}(xy)$$

where tr is the trace mapping from V to F. Let $T: V \to V$ be the F-linear map defined by $T(b) = ab$. Since $B(T(x), y)) = B(x, T(y))$, T is self-adjoint with respect to the symmetric bilinear form B. By our choice of a, B is positive definite with respect to every possible ordering of F. In other words, in any diagonal representation of B, every diagonal entry must be a sum of squares in F and therefore a square as F is pythagorean. With this, one can choose a basis for V so that the matrix for B with respect to this basis is the identity matrix. Letting S represent the matrix of T relative to this basis, the self-adjoint behavior of T implies that S is symmetric. By construction, a is an eigenvalue of T and therefore an eigenvalue of S. □

The proof of this theorem shows that if $a \in R(F)$ has degree n over F then a is an eigenvalue of some symmetric $n \times n$ matrix. For a more general field F and $a \in R(F)$ it is interesting to ask what size of symmetric matrix is required to have a as an eigenvalue. For example, for the field $\mathbb{Q}$ of rational numbers, $R(\mathbb{Q})$ is the set of real algebraic numbers. In [**1**], E. Bender showed that every real algebraic number of degree n is an eigenvalue of some symmetric $(n + 1) \times (n + 1)$ matrix over $\mathbb{Q}$. The analogous question for algebraic integers as eigenvalues of symmetric integer matrices has been considered by D. Estes [**4**].

With this result we can now give a complete characterization of the fields for which the Principal Axis Property holds.

Theorem 4. *A field F satisfies the Principal Axis Property if and only if F is an intersection of real closed fields.*

Proof: The "if" part is established by the Corollary to Theorem 2. To continue, let $a \in R(F)$. Choosing a symmetrix matrix over F having a as an eigenvalue, we see that $a \in F$ by hypothesis. Thus $F = R(F)$ and the characterization is complete. □

ACKNOWLEDGMENTS. The authors wish to thank E. Becker and A. Wadsworth for their help in revising this paper. Their interest and suggestions are greatly appreciated.

REFERENCES

1. E. A. Bender, The dimensions of symmetric matrices with a given minimum polynomial, *Linear Alg. Appl.* 3 (1970) 115–123.
2. A. Charnow and E. Charnow, Fields for which the principal axis theorem is valid, *Math. Mag.* 59 (1986) 222–225.
3. T. Craven, Intersections of real closed fields, *Can. J. Math.* 32 (1980) 431–440.
4. D. Estes, Eigenvalues of symmetric integer matrices, (preprint 1991).
5. S. H. Freidberg, Extending the principal axis theorem to fields other than $\mathbb{R}$, *Amer. Math. Monthly* 97 (1990) 147–149.
6. F. Krakowski, Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern, *Comment. Math. Helv.* 32 (1958) 224–240.
7. T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin Publ. Co., Reading, MA, 1973.
8. W. Scharlau, *Quadratic and Hermitian Forms*, Springer Verlag, Berlin-Heidelberg-New York-Tokyo, 1985.
9. B. L. van der Waerden, *Algebra, vol. 2*, Frederick Ungar Publ. Co., New York, 1970.
10. W. Waterhouse, Self-adjoint operators and formally real fields, *Duke Math. J.* 43 (1976) 237–243.

Department of Mathematics
Colgate University
Hamilton, NY 13346

Department of Mathematics
Ohio State University
Columbus, OH 43210

Department of Mathematics
Colgate University
Hamilton, NY 13346

THE CHAUVENET PRIZE.

The committee on the award of the first Chauvenet Prize for excellence in mathematical exposition, Professors W. C. GRAUSTEIN, ANNA PELL WHEELER, and A. B. VAN VLECK, chairman, recommended that the award be made to Professor G. A. BLISS of the University of Chicago for his paper on "Algebraic functions and their divisors," published in the *Annals of Mathematics*, v lume 26, Numbers 1 and 2, September and December 1924. The Trustees voted to approve this choice and to thank the members of the committee for their arduous but vĕry valuable efforts. The award was announced at the business meeting and the prize of one hundred dollars, furnished by a member of the Association, was presented to Professor Bliss following the meetings.

33(1926), 177

The Fifty-Third William Lowell Putnam Mathematical Competition

Leonard F. Klosinski
Gerald L. Alexanderson
Loren C. Larson

The following results of the fifty-third William Lowell Putnam Mathematical Competition, held on December 5, 1992, have been determined in accordance with the governing regulations. This annual contest is supported by the William Lowell Putnam Prize Fund for the Promotion of Scholarship, left by Mrs. Putnam in memory of her husband, and is held under the auspices of the Mathematical Association of America.

The first prize, $7,500, was awarded to the Department of Mathematics of Harvard University. The members of the winning team were: Jordan S. Ellenberg, Samuel A. Kutin, and Royce Y. Peng; each was awarded a prize of $500.

The second prize, $5,000, was awarded to the Department of Mathematics of the University of Toronto. The members of the winning team were: J. P. Grossman, Jeff T. Higham, and Hugh R. Thomas; each was awarded a prize of $400.

The third prize, $3,000, was awarded to the Department of Mathematics of the University of Waterloo. The members of the winning team were Dorian Birsan, Daniel R. L. Brown, and Ian A. Goldberg; each was awarded a prize of $300.

The fourth prize, $2,000, was awarded to the Department of Mathematics at Princeton University. The members of the winning team were Joshua B. Fischman, Adam M. Logan, and Joel E. Rosenberg; each was awarded a prize of $200.

The fifth prize, $1,000, was awarded to the Department of Mathematics at Cornell University. The members of the winning team were Jon M. Kleinberg, Mark Krosky, and Demetrio A. Muñoz; each was awarded a prize of $100.

The five highest ranking individual contestants, in alphabetical order, were Jordan S. Ellenberg, Harvard University; Samuel A. Kutin, Harvard University; Adam M. Logan, Princeton University; Serban M. Nacu, Harvard University; and Jeffrey M. Vanderkam, Duke University. Each of these was designated a Putnam Fellow by the Mathematical Association of America and awarded a prize of $1,000 by the Putnam Prize Fund.

The next six highest ranking contestants, in alphabetical order, were David B. Carlton, Harvard University; Ian A. Goldberg, University of Waterloo; Kiran S. Kedlaya, Harvard University; Royce Y. Peng, Harvard University; Hugh R. Thomas, University of Toronto; and Tong Zhang, Cornell University; each was awarded a prize of $500.

The next four highest ranking individuals, in alphabetical order, were Ze-Yu Chen, Princeton University; Jonathan T. Higa, Princeton University; Svetlozar E. Nestorov, Stanford University; and Samuel K. Vandervelde, Swarthmore College; each was awarded a prize of $250.

The next nine highest ranking individuals, in alphabetical order, were Daniel R. L. Brown, University of Waterloo; Jeff T. Higham, University of Toronto; F. Dean Hildebrandt, Harvard University; Julie B. Kerr, Washington State University; Andrew H. Kresch, Yale University; William R. Mann, Princeton University; Dana Pascovici, Dartmouth College; Michail G. Sunitsky, Princeton University; and Douglas J. Zare, New College of the University of South Florida; each was awarded a prize of $100.

The following teams, named in alphabetical order, received honorable mention: Dartmouth College, with team members Radu Bacioiu, Rolf H. Nelson, and Dana Pascovici; Duke University, with team members Craig B. Gentry, Alexander J. Hartemink, and Jeffrey M. Vanderkam; Massachusetts Institute of Technology, with team members Thomas C. Chou, Henry L. Cohn, and Michael J. Lawler; University of British Columbia, with team members Malik H. Kalfane, David L. Savitt, and Mark A. Van Raamsdonk; and Yale University, with team members Thomas Feng, Andrew H. Kresch, and Zhaohui Zhang.

Honorable mention was achieved by the following thirty-one individuals named in alphabetical order: James McCleery Berger, Brown University; Sergey Brin, University of Maryland, College Park; Thomas C. Chou, Massachusetts Institute of Technology; Henry L. Cohn, Massachusetts Institute of Technology; Brian D. Ewald, University of Michigan, Ann Arbor; Joshua B. Fischman, Princeton University; J. P. Grossman, University of Toronto; Steven S. Gubser, Princeton University; William M. Hesse, University of Connecticut; Adam Kalai, Harvard University; Timothy P. Kokesh, Harvey Mudd College; Botond Kőszegi, Harvard University; Peter R. Kramer, Princeton University; Mark Krosky, Cornell University; Tal N. Kubo, Harvard University; Sergey V. Levin, Harvard University; Samuel J. Maltby, University of Calgary; Demetrio A. Muñoz, Cornell University; Akira Negi, University of North Carolina, Chapel Hill; Seth Padowitz, Brown University; Andrew Przeworski, Massachusetts Institute of Technology; Philip T. Reiss, University of Manitoba; James P. Sarvis, Massachusetts Institute of Technology; Kannan Soundararajan, University of Michigan, Ann Arbor; Michael G. Szydlo, Boston University; Joe Y. Tien, University of California, Irvine; Mark A. Van Raamsdonk, University of British Columbia; Jeffrey D. Wall, Princeton University; Kelly Lynne Wieand, University of Wisconsin, Madison; Erick B. Wong, Simon Fraser University; and Zhaohui Zhang, Yale University.

The other individuals who achieved ranks among the top 98, in alphabetical order of their schools, were: Brigham Young University, John Wesley Robertson; University of British Columbia, David L. Savitt; Brown University, Andrew Brecher; California Institute of Technology, Steven C. Anderson; University of California, Berkeley, Daniel C. Isaksen; University of Colorado, Boulder, Steve T. Soulé; Cornell University, Jon M. Kleinberg; Dartmouth College, Radu Bacioiu; Duke University, Alexander J. Hartemink; Harvard University, Manjul Bhargava, Joseph I. Chuang, Michael L. Hutchings, Dimitri Kountourogiannis, Paul Li, Matteo J. Paris, Chris Ternoey; Harvey Mudd College, Jon H. Leonard; University of Maine, Orono, YuQun Chen; Massachusetts Institute of Technology, Jerome S. Khohayting, Tichomir G. Tenev, William W. Tucker; Memorial University of Newfoundland, Robert P. Gallant; Michigan State University, Thomas P. Hayes; University of Minnesota, Minneapolis, Matthew P. Kelly; Université de Montréal, Marc-André

Lafortune; New York University, Mikhail Kogan; Ohio State University, Frank J. Swenton; University of Pennsylvania, Frosti Petursson; Princeton University, Tibor Beke, Mark W. Lucianovic; Purdue University, Pok-Yin Yu; Rice University, Donald A. Barkauskas; Rose Hulman Institute of Technology, Jonathan E. Atkins; Stanford University, Daniel P. Cory, Garrett R. Vargas; Texas A & M University, Zheng-Zheng Li; University of Waterloo, Dorian Birsan, Kevin K. Cheung, Jie J. Lou; Wellesley College, Yihao L. Zhang; West Virginia Wesleyan College, Emanuel V. Todorov; and Yale University, Matthew Frank.

The Elizabeth Lowell Putnam Prize, named for the wife of William Lowell Putnam and to be "awarded periodically to a woman whose performance on the Competition has been deemed particularly meritorious", is awarded this year for the first time to Dana Pascovici of Dartmouth College. The winner is awarded a prize of $500.

There were 2421 individual contestants from 393 colleges and universities in Canada and the United States in the competition of December 5, 1992. Teams were entered by 284 institutions.

The Questions Committee for the fifty-third competition consisted of George E. Andrews (Chair), George T. Gilbert, and Eugene Luks; they composed the problems listed below and were most prominent among those suggesting solutions.

PROBLEMS

Problem A-1.

Prove that $f(n) = 1 - n$ is the only integer-valued function defined on the integers that satisfies the following conditions:

(i) $f(f(n)) = n$, for all integers n;
(ii) $f(f(n+2)+2) = n$ for all integers n;
(iii) $f(0) = 1$.

Problem A-2.

Define $C(\alpha)$ to be the coefficient of x^{1992} in the power series expansion about $x = 0$ of $(1+x)^{\alpha}$. Evaluate

$$\int_0^1 C(-y-1)\left(\frac{1}{y+1} + \frac{1}{y+2} + \frac{1}{y+3} + \cdots + \frac{1}{y+1992}\right) dy.$$

Problem A-3.

For a given positive integer m, find all triples (n, x, y) of positive integers, with n relatively prime to m, which satisfy $(x^2 + y^2)^m = (xy)^n$.

Problem A-4.

Let f be an infinitely differentiable real-valued function defined on the real numbers. If

$$f\left(\frac{1}{n}\right) = \frac{n^2}{n^2+1}, \qquad n = 1,2,3,\ldots,$$

compute the values of the derivatives $f^{(k)}(0)$, $k = 1,2,3,\ldots$.

Problem A-5.

For each positive integer n, let

$$a_n = \begin{cases} 0 & \text{if the number of 1's in the binary representation of } n \text{ is even,} \\ 1 & \text{if the number of 1's in the binary representation of } n \text{ is odd.} \end{cases}$$

Show that there do not exist positive integers k and m such that

$$a_{k+j} = a_{k+m+j} = a_{k+2m+j}, \quad \text{for } 0 \le j \le m-1.$$

Problem A-6.

Four points are chosen at random on the surface of a sphere. What is the probability that the center of the sphere lies inside the tetrahedron whose vertices are at the four points? (It is understood that each point is independently chosen relative to a uniform distribution on the sphere.)

Problem B-1.

Let S be a set of n distinct real numbers. Let A_S be the set of numbers that occur as averages of two distinct elements of S. For a given $n \ge 2$, what is the smallest possible number of distinct elements in A_S?

Problem B-2.

For nonnegative integers n and k, define $Q(n,k)$ to be the coefficient of x^k in the expansion of $(1 + x + x^2 + x^3)^n$. Prove that

$$Q(n,k) = \sum_{j=0}^{n} \binom{n}{j}\binom{n}{k-2j},$$

where $\binom{a}{b}$ is the standard binomial coefficient. (Reminder: For integers a and b with $a \ge 0$, $\binom{a}{b} = a!/(b!(a-b)!)$ for $0 \le b \le a$, and $\binom{a}{b} = 0$ otherwise.)

Problem B-3.

For any pair (x, y) of real numbers, a sequence $(a_n(x,y))_{n\ge 0}$ is defined as follows:

$$a_0(x,y) = x,$$

$$a_{n+1}(x,y) = \frac{(a_n(x,y))^2 + y^2}{2}, \quad \text{for all } n \ge 0.$$

Find the area of the region $\{(x,y) \mid (a_n(x,y))_{n\ge 0} \text{ converges}\}$.

Problem B-4.

Let $p(x)$ be a nonzero polynomial of degree less than 1992 having no nonconstant factor in common with $x^3 - x$. Let

$$\frac{d^{1992}}{dx^{1992}}\left(\frac{p(x)}{x^3 - x}\right) = \frac{f(x)}{g(x)}$$

for polynomials $f(x)$ and $g(x)$. Find the smallest possible degree of $f(x)$.

Problem B-5.

Let D_n denote the value of the $(n-1) \times (n-1)$ determinant

$$\begin{vmatrix} 3 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 4 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 5 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 6 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & n+1 \end{vmatrix}.$$

Is the set $\{D_n/n!\}_{n \geq 2}$ bounded?

Problem B-6.

Let $\mathcal{M}$ be a set of real $n \times n$ matrices such that

(i) $I \in \mathcal{M}$, where I is the $n \times n$ identity matrix;
(ii) if $A \in \mathcal{M}$ and $B \in \mathcal{M}$, then either $AB \in \mathcal{M}$ or $-AB \in \mathcal{M}$, but not both;
(iii) if $A \in \mathcal{M}$ and $B \in \mathcal{M}$, then either $AB = BA$ or $AB = -BA$;
(iv) if $A \in \mathcal{M}$ and $A \neq I$, there is at least one $B \in \mathcal{M}$ such that $AB = -BA$.

Prove that $\mathcal{M}$ contains at most n^2 matrices.

SOLUTIONS

In the 12-tuples $(n_{10}, n_9, \ldots, n_0, n_{-1})$ following each problem number below, n_i for $10 \geq i \geq 0$ is the number of students among the top 203 contestants achieving i points for the problem and n_{-1} is the number of those not submitting solutions.

A – 1 (31, 82, 42, 10, 0, 0, 0, 7, 23, 6, 2, 0)

Solution. If $f(n) = 1 - n$, then $f(f(n)) = f(1 - n) = 1 - (1 - n) = n$, so (i) holds. Similarly, $f(f(n + 2) + 2) = f((-n - 1) + 2) = f(1 - n) = n$, so (ii) holds. Clearly (iii) holds, and so $f(n) = 1 - n$ satisfies the conditions.

Conversely, suppose f satisfies the three given conditions. From condition (ii), $f(f(f(n + 2) + 2)) = f(n)$, and applying (i) yields $f(n + 2) + 2 = f(n)$ or $f(n +$

2) $= f(n) - 2$. An easy induction yields

$$f(n) = \begin{cases} f(0) - n & \text{if } n \text{ is even,} \\ f(1) + 1 - n & \text{if } n \text{ is odd.} \end{cases}$$

If $f(0) = 1$, then $f(1) = 0$ by (i), therefore, $f(n) = 1 - n$.

A-2 (157, 1, 0, 0, 0, 0, 0, 0, 2, 14, 14, 15)

Solution. From the binomial series, we see that

$$C(-y-1) = \frac{(-y-1)(-y-2)\cdots(-y-1992)}{1992!}$$
$$= \frac{(y+1)(y+2)\cdots(y+1992)}{1992!}.$$

Therefore,

$$C(-y-1)\left(\frac{1}{y+1} + \frac{1}{y+2} + \cdots + \frac{1}{y+1992}\right)$$
$$= \frac{d}{dy}\left(\frac{(y+1)(y+2)\cdots(y+1992)}{1992!}\right).$$

Hence the integral in question is

$$\int_0^1 \frac{d}{dy}\left(\frac{(y+1)(y+2)\cdots(y+1992)}{1992!}\right)dy = \left.\frac{(y+1)(y+2)\cdots(y+1992)}{1992!}\right|_0^1$$
$$= 1993 - 1 = 1992.$$

A-3 (55, 20, 7, 0, 0, 0, 0, 0, 16, 7, 45, 53)

Solution. There are no solutions if m is odd. If m is even, the only solution is $(n, x, y) = (m+1, 2^{m/2}, 2^{m/2})$.

If (n, x, y) is a solution, then by the arithmetic-mean—geometric-mean inequality, $(xy)^n = (x^2 + y^2)^m \geq (2xy)^m$, so $n > m$. Let p be a prime number. Let a and b be the largest powers of p that divide x and y, respectively. Then the largest power of p dividing $(xy)^n$ is $(a+b)n$. If $a < b$, the largest power of p dividing $(x^2 + y^2)^m$ is $2am$. But this implies that $(a+b)n = 2am$, and this contradicts $n > m$. Similarly, the assumption $a > b$ leads to a contradiction. Therefore $a = b$ for all primes p, and we conclude that $x = y$. Thus, the equation reduces to $(2x^2)^m = x^{2n}$, or equivalently, $x^{2(n-m)} = 2^m$. It follows that x is a positive power of 2, say 2^a. This implies $2(n-m)a = m$, or, $2an = (2a+1)m$. Since $\gcd(m, n) = \gcd(2a, 2a+1) = 1$, we must have $m = 2a$ and $n = 2a+1$. Thus, m is necessarily even and the solution follows as claimed.

A-4 (17, 6, 7, 0, 0, 0, 2, 0, 73, 18, 47, 33)

Solution. We will show that

$$f^{(k)}(0) = \begin{cases} (-1)^{k/2}k! & \text{if } k \text{ is even,} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

First we note that if $h(x)$ is a differentiable function and $x_1, x_2, \ldots,$ is a sequence strictly decreasing to 0 such that $h(x_n) = 0$, then by Rolle's Theorem, there exists a sequence $y_1, y_2, \ldots,$ strictly decreasing to 0, such that $h'(y_n) = 0$ $(x_{n+1} < y_n < x_n)$.

Now let $g(x) = f(x) - 1/(1 + x^2)$. Then $g(1/n) = 0$ for $n = 1, 2, \ldots$. Applying the result of the preceding paragraph to $g, g', g'', \ldots$ and invoking the continuity of $g^{(k)}$ at 0, we see that $g^{(k)}(0) = 0$ for $k = 0, 1, 2, 3, \ldots$. Thus,

$$f^{(k)}(0) = \frac{d^k}{dx^k}\left(\frac{1}{1 + x^2}\right)\bigg|_{x=0}.$$

The Maclaurin series for $1/(1 + x^2)$ is $\sum_{k=0}^{\infty}(-1)^k x^{2k}$, and hence $f^{(k)}(0)$ is equal to the values given above.

A-5 (1, 9, 1, 0, 0, 0, 0, 0, 5, 3, 72, 112)

Solution. Observe that $a_{2n} = a_n$ and $a_{2n+1} = 1 - a_{2n} = 1 - a_n$.

Suppose that there exist k, m as above, and we may assume m is minimal for such.

Suppose first that m is odd. We'll suppose $a_k = a_{k+m} = a_{k+2m} = 0$, as it will be clear that the case $a_k = 1$ can be treated similarly. Since either k or $k + m$ is even, $a_{k+1} = a_{k+m+1} = a_{k+2m+1} = 1$. Again, since either $k + 1$ or $k + m + 1$ is even, $a_{k+2} = a_{k+m+2} = a_{k+2m+2} = 0$. By this means, we see that the terms $a_k, a_{k+1}, a_{k+2}, \ldots, a_{k+m-1}$ alternate between 0 and 1. Then since $m - 1$ is even, $a_{k+m-1} = a_{k+2m-1} = a_{k+3m-1} = 0$. But, since either $k + m - 1$ or $k + 2m - 1$ is even, that would imply that $a_{k+m} = a_{k+2m} = 1$, a contradiction.

Thus, m must be even. Extracting the terms with even indices in

$$a_{k+j} = a_{k+m+j} = a_{k+2m+j}, \quad \text{for } 0 \le j \le m - 1,$$

and using the fact that $a_r = a_{r/2}$ for even r, we get

$$a_{\lceil k/2 \rceil + i} = a_{\lceil k/2 \rceil + (m/2) + i} = a_{\lceil k/2 \rceil + m + i}, \quad \text{for } 0 \le i \le (m/2) - 1.$$

(The even numbers $\ge k$ are $2\lceil k/2 \rceil, 2\lceil k/2 \rceil + 2, \ldots$.) This contradicts the minimality of m.

Hence, there are no such k and m.

A-6 (9, 3, 4, 0, 0, 0, 0, 0, 0, 10, 32, 22, 123)

Solution. Recall first that if points A, B, C, D are in general position in 3-space, then a point E lies inside the tetrahedron $ABCD$ if and only if the barycentric coordinates of E with respect to A, B, C, D are positive. That is, if we (uniquely) express

$$\vec{E} = w\vec{A} + x\vec{B} + y\vec{C} + z\vec{D}, \quad \text{with } w + x + y + z = 1,$$

(the arrows indicating consideration of the coordinate triples as vectors), then E is in the interior of $ABCD$ if and only if $w > 0$, $x > 0$, $y > 0$, and $z > 0$. Hence, if E is the origin, then E is in the interior of $ABCD$ if and only if there is a solution (w, x, y, z) to

$$\vec{0} = w\vec{A} + x\vec{B} + y\vec{C} + z\vec{D} \tag{1}$$

with w, x, y, z having the same sign. As the solution space to (1) is 1-dimensional, this condition holds for one nonzero solution if and only if it holds for all.

Now assume that the center of the sphere is located at the origin and fix the first chosen point P on the sphere as the north pole, the other three points, P_1, P_2, P_3, then being random.

We may suppose the choice of each P_i is made in two steps, the first choosing a random diameter $Q_{i_1}Q_{i_2}$ and the second choosing at random between the endpoints Q_{i_1}, Q_{i_2}. Since the $2^3 = 8$ possible selections of endpoints of the three diameters are equally likely, each of the 8 tetrahedra $PQ_{1j_1}Q_{2j_2}Q_{3j_3}$, $j_i = 1$ or 2, are equally likely. We may further suppose that the vertices of each of these tetrahedra are in general position as the probability of degeneracy is 0. Similarly, we may suppose that the center of the sphere does not lie on any face of the tetrahedra.

Let (w, x, y, z) be a nonzero solution to the equation

$$\vec{0} = w\vec{P} + x\vec{Q}_{11} + y\vec{Q}_{21} + z\vec{Q}_{31}.$$

Then, since $\vec{Q}_{i1} = -\vec{Q}_{i2}$, the eight equations

$$\vec{0} = w\vec{P} + x\vec{Q}_{1j_1} + y\vec{Q}_{2j_2} + z\vec{Q}_{3j_3}$$

have respective solutions

$$(w, x, y, z), (w, x, y, -z), (w, x, -y, z), (w, -x, y, z),$$

$$(w, x, -y, -z), (w, -x, -y, z), (w, -x, y, -z), (w, -x, -y, -z).$$

Hence, exactly one of the eight equations has a solution whose coordinates have the same sign.

It follows that exactly one of these 8 equally likely tetrahedra contains the center. Thus the probability of including the center is $1/8$ for all initial choices of 3 diameters. We conclude that the probability for a random tetrahedron is $1/8$.

B-1 (145, 15, 4, 0, 0, 0, 0, 0, 0, 6, 14, 11, 8)

Solution. The smallest possible number of elements in A_S is $2n - 3$.

Let $x_1 < x_2 < \cdots < x_n$ represent the elements of S. Then

$$\frac{x_1 + x_2}{2} < \frac{x_1 + x_3}{2} < \cdots < \frac{x_1 + x_n}{2} < \frac{x_2 + x_n}{2} < \frac{x_3 + x_n}{2}$$
$$< \cdots < \frac{x_{n-1} + x_n}{2}$$

represent $(n - 1) + (n - 2) = 2n - 3$ distinct elements of A_S, so A_S has at least $2n - 3$ distinct elements.

On the other hand, if we take $S = \{1, 2, \ldots, n\}$, the elements of A_S are $\frac{3}{2}, \frac{4}{2}, \frac{5}{2}, \ldots, \frac{2n-1}{2}$. There are only $(2n - 1) - 2 = 2n - 3$ such numbers; thus there is a set A_S with at most $2n - 3$ distinct elements. This completes the proof.

B-2 (159, 10, 7, 0, 0, 0, 0, 0, 1, 4, 13, 9)

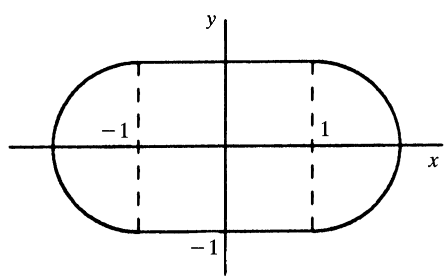
Solution. We have

$$\begin{aligned}\sum_{k\geq 0} Q(n,k)x^k &= (1+x+x^2+x^3)^n \\ &= (1+x^2)^n(1+x)^n \\ &= \sum_{j\geq 0}\binom{n}{j}x^{2j}\sum_{i\geq 0}\binom{n}{i}x^i \\ &= \sum_{j\geq 0}\sum_{i\geq o}x^{2j+i}\binom{n}{j}\binom{n}{i} \\ &= \sum_{k\geq 0}x^k\sum_{j\geq 0}\binom{n}{j}\binom{n}{k-2j}.\end{aligned}$$

Comparing coefficients of x^k, we derive the desired result.

B-3 (23, 11, 10, 0, 0, 0, 0, 0, 27, 24, 71, 37)

Solution. The area is $4+\pi$. The region of convergence is



namely, a (closed) square $\{(x,y) | -1 \leq x, y \leq 1\}$ of side 2 with (closed) semicircles of radius 1 centered at $(\pm 1, 0)$ described on two opposite sides.

If $\lim_{n\to\infty} a_n(x,y) = L$, then L must satisfy $L = (L^2+y^2)/2$; that is, L must be a root of the equation

$$r^2 - 2r + y^2 = 0. \tag{1}$$

In such case, the equation must have real roots, so the discriminant, $4-4y^2$, must be nonnegative. Thus, a necessary condition for $(a_n(x,y))$ to converge is that $|y| \leq 1$.

Fix $|y| \leq 1$. The roots of (1) are then $1-\sqrt{1-y^2}$ and $1+\sqrt{1-y^2}$, which are real and nonnegative. As $a_1(-x,y) = a_1(x,y)$, the interval of convergence is symmetric about $x=0$. We shall assume then that $x \geq 0$; thus, $a_n(x,y) \geq 0$, for all n.

If $r_0 = 1 \pm \sqrt{1-y^2}$, then $a_{n+1}(x,y)$ is less than, equal to, or greater than r_0 according to whether $a_n(x,y)$ is less than, equal to, or greater than r_0 $(= (r_0^2+y^2)/2)$.

If $a_n(x, y)$ lies in the closed interval $[1 - \sqrt{1-y^2}, 1 + \sqrt{1-y^2}]$, that is, between the roots of (1), then

$$a_n(x,y)^2 - 2a_n(x,y) + y^2 \le 0,$$

so that

$$1 - \sqrt{1-y^2} \le a_{n+1}(x,y) \le a_n(x,y).$$

It follows that $(a_n(x, y))_{n\ge 0}$ converges if x is in the closed interval $[1 - \sqrt{1-y^2}, 1 + \sqrt{1-y^2}]$.

If $a_n(x, y)$ does not lie in the interval $[1 - \sqrt{1-y^2}, 1 + \sqrt{1-y^2}]$, then

$$a_n(x,y)^2 - 2a_n(x,y) + y^2 > 0,$$

so that

$$a_{n+1}(x,y) > a_n(x,y).$$

Thus, if x, and therefore all $a_n(x, y)$, are greater than $1 + \sqrt{1-y^2}$, then the sequence diverges. On the other hand, if x, and therefore all $a_n(x, y)$, lie between 0 and $1 - \sqrt{1-y^2}$, the sequence converges monotonically to $1 - \sqrt{1-y^2}$.

To summarize, $(a_n(x, y))_{n\ge 0}$ converges if and only if

$$-1 \le y \le 1$$

and

$$-\left(1 + \sqrt{1-y^2}\right) \le x \le 1 + \sqrt{1-y^2}.$$

B-4 (35, 11, 13, 0, 0, 0, 0, 0, 12, 5, 48, 79)

Solution. The smallest possible degree of $f(x)$ is 3984.

By the Division Algorithm, we can write $p(x) = (x^3 - x)q(x) + r(x)$, where $q(x)$ and $r(x)$ are polynomials, the degree of $r(x)$ is less than 3, and the degree of $q(x)$ is less than 1989. Then

$$\frac{d^{1992}}{dx^{1992}}\left(\frac{p(x)}{x^3-x}\right) = \frac{d^{1992}}{dx^{1992}}\left(\frac{r(x)}{x^3-x}\right).$$

Now, write $r(x)/(x^3 - x)$ in the form

$$\frac{A}{x-1} + \frac{B}{x} + \frac{C}{x+1}.$$

Because $p(x)$ and $x^3 - x$ have no nonconstant common factor, neither do $r(x)$ and $x^3 - x$, and therefore, $ABC \ne 0$. Thus,

$$\begin{aligned}
&\frac{d^{1992}}{dx^{1992}}\left(\frac{r(x)}{x^3-x}\right)\\
&\quad= 1992!\left(\frac{A}{(x-1)^{1993}} + \frac{B}{x^{1993}} + \frac{C}{(x+1)^{1993}}\right)\\
&\quad= 1992!\left(\frac{Ax^{1993}(x+1)^{1993} + B(x-1)^{1993}(x+1)^{1993} + C(x-1)^{1993}x^{1993}}{(x^3-x)^{1993}}\right).
\end{aligned}$$

Since $ABC \neq 0$, it is clear that the numerator and denominator have no common factor. Expanding the numerator yields an expression of the form

$$(A + B + C)x^{3986} + 1993(A - C)x^{3985} + 1993(996A - B + 996C)x^{3984} + \cdots .$$

From $A = C = 1$, $B = -2$, we see the degree can be as low as 3984. A lower degree would imply $A + B + C = 0$, $A - C = 0$, $996A - B + 996C = 0$, implying that $A = B = C = 0$, a contradiction.

B-5 (62, 4, 4, 0, 0, 0, 0, 3, 6, 2, 49, 73)

Solution 1. The set $\{D_n/n!\}_{n \geq 2}$ forms a sequence which strictly increases to infinity; it is therefore unbounded.

Observing that $D_2 = 3$ and $D_3 = 11$, we obtain a recursion for D_{n+1}. Subtracting the next-to-last column from the last column and then the next-to-last row from the last row, one finds

$$D_{n+1} = \det \begin{pmatrix} 3 & 1 & 1 & \cdots & & 1 & 0 \\ 1 & 4 & 1 & \cdots & & 1 & 0 \\ 1 & 1 & 5 & \cdots & & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 & n+1 & -n \\ 0 & 0 & 0 & \cdots & 0 & -n & 2n+1 \end{pmatrix}.$$

Expanding the determinant in its last row, one obtains

$$D_{n+1} = (2n + 1)D_n - n^2 D_{n-1}.$$

Letting $r_n = (D_n/n!)$, the recursion may be written as

$$r_{n+1} = \frac{2n+1}{n+1} r_n - \frac{n}{n+1} r_{n-1},$$

or

$$(r_{n+1} - r_n) = \frac{n}{n+1}(r_n - r_{n-1}).$$

We conclude that

$$r_{n+1} - r_n = \frac{3}{n+1}(r_3 - r_2) = \frac{1}{n+1}.$$

Therefore,

$$\begin{aligned} r_{n+1} &= r_2 + (r_3 - r_2) + (r_4 - r_3) + \cdots + (r_{n+1} - r_n) \\ &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n+1}, \end{aligned}$$

so the sequence (r_n) diverges to infinity.

Solution 2. The problem is the case $a_i = i + 1$ of

$$D_{n+1}(a_1,\dots,a_n) = \det\begin{pmatrix} 1+a_1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 1+a_2 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1+a_3 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 1+a_4 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & 1+a_n \end{pmatrix}$$

$$= \prod_{i=1}^{n} a_i + \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} a_j.$$

This formula follows immediately from the recurrence

$$D_{n+1}(a_1,\dots,a_n) = a_n D_n(a_1,\dots,a_{n-1}) + a_{n-1} D_n(a_1,\dots,a_{n-2},0).$$

To prove this recurrence, subtract the $(n-1)$st column from the nth column, and then expand along the nth column.

If none of the a_i's equal 0, we can write the polynomial $D_n(a_1,\dots,a_{n-1})$ in the form

$$D_n(a_1,\dots,a_{n-1}) = a_1 a_2 \cdots a_{n-1}\left(1 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_{n-1}}\right).$$

It follows that

$$\frac{D_n}{n!} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n},$$

so the sequence $(D_n/n!)$ is unbounded.

B-6 (0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 4, 39, 155)

Solution 1. We prove the result more generally for complex matrices (because it is convenient to use $i = \sqrt{-1}$ in the proof).

The proof is by induction on n.

If $n = 1$ then the elements of $\mathscr{M}$ commute so that (iv) cannot be satisfied unless $\mathscr{M} = \{I\}$. Suppose that $n > 1$ and that the result holds for sets of complex matrices of smaller dimension.

We may assume $|\mathscr{M}| > 1$, so by (iv), there exist $C, D \in \mathscr{M}$ with $CD = -DC$. Fix such C, D. As in the first solution, $C^2 = \pm I$. Hence the eigenvalues of C are $\pm\lambda$ where $\lambda = 1$ or i. Furthermore, $\mathbf{C}^n = V_\lambda \oplus V_{-\lambda}$, where $V_\lambda, V_{-\lambda}$ are the nullspaces of $(C - \lambda I), (C + \lambda I)$ respectively. We observe that if $X \in \mathscr{M}$ then

$$CX = XC \Rightarrow (C \pm \lambda I)X = X(C \pm \lambda I) \Rightarrow V_{\pm\lambda}X = V_{\pm\lambda};$$

$$CX = -XC \Rightarrow (C \pm \lambda I)X = (-1)X(C \mp \lambda I) \Rightarrow V_{\pm\lambda}X = V_{\mp\lambda}.$$

In particular, since $V_\lambda D = V_{-\lambda}$, $\dim(V_\lambda) = \dim(V_{-\lambda}) = n/2$.

Let $\mathscr{N} = \{X \in \mathscr{M} \mid CX = XC,\ DX = XD\}$. If $Y \in \mathscr{M}$ then exactly one of Y, YC, YD, YCD is in $\mathscr{N}$. It follows that $|\mathscr{N}| = |\mathscr{M}|/4$.

For $X \in \mathscr{N}$, let $\phi(X)$ be the $n/2 \times n/2$ matrix representing, with respect to a fixed basis of V_λ, the linear transformation given by $v \to vX$ for $v \in V_\lambda$. Then ϕ is injective. To see this: assume $\phi(X) = \phi(Y)$ so that $vX = vY$ for $v \in V_\lambda$; but if $v \in V_{-\lambda}$ then $vD \in V_\lambda$, so that $vXD = vDX = vDY = vYD$, which again implies

$vX = vY$; since X, Y induce the same transformations of both V_λ and $V_{-\lambda}$, it follows that $X = Y$.

If suffices finally to show that $\phi(\mathscr{N})$, a set of $n/2 \times n/2$ complex matrices, satisfies (i), (ii), (iii), (iv), for then, by induction, $|\phi(\mathscr{N})| \le (n/2)^2$, whence $|\mathscr{M}| = 4|\mathscr{N}| = 4|\phi(\mathscr{N})| \le n^2$.

Conditions (i), (ii), (iii) for $\phi(\mathscr{N})$ are clearly inherited from those of $\mathscr{M}$. To show (iv), let $\phi(A) \in \phi(\mathscr{N})$, with $\phi(A)$ not the $n/2 \times n/2$ identity matrix. Then $A \ne I$ (as ϕ is injective) and $AB = -BA$ for some $B \in \mathscr{M}$. Let B' be the element of $\{B, BC, BD, BCD\}$ belonging to $\mathscr{N}$. Since $AB' = -B'A$, $\phi(A)\phi(B') = -\phi(B')\phi(A)$.

Solution 2. Let G be the group $\{\pm A \mid A \in \mathscr{M}\}$. We must show that $|G| \le 2n^2$.

The center of G, $Z(G)$, consists of $\pm I$, and if $X \in G \setminus Z(G)$, then X has precisely two conjugates, namely itself and $-X$. Thus G has $1 + |G|/2$ conjugacy classes, and therefore, G has $1 + |G|/2$ inequivalent irreducible representations over $\mathbf{C}$.

The number of inequivalent representations of dimension 1 is $|G/G'|$, where G' is the commutator subgroup. Since $G' = \{\pm I\} = Z(G)$, this number is $|G|/2$.

The remaining irreducible representation then has dimension $\sqrt{|G|/2}$ (since the sum of the squares of the dimensions of the irreducible representations is $|G|$). This representation must be contained in the given representation of G in $n \times n$ matrices, for in all the 1-dimensional representations, $Z(G)$ is in the kernel. Hence $n \ge \sqrt{|G|/2}$, or $2n^2 \ge |G|$.

Klosinski:
Department of Mathematics
Santa Clara University
Santa Clara, CA 95053

Alexanderson:
Department of Mathematics
Santa Clara University
Santa Clara, CA 95053

Larson:
Department of Mathematics
St. Olaf College
Northfield, MN 55057

A Visual Explanation of Jensen's Inequality

Tristan Needham

"This theorem is so fundamental that we propose to give a number of proofs, of varying degrees of simplicity and generality." So say Hardy, Littlewood, and Pólya ([**1**], p. 17) of the theorem of the arithmetic and geometric means. True to their word, they proceed to give eleven (!) different proofs of the fact that for non-negative x_i,

$$\sqrt[n]{x_1 \cdot x_2 \cdots x_n} \leq \left(\frac{x_1 + x_2 + \cdots + x_n}{n}\right), \tag{1}$$

with equality *iff* $x_1 = x_2 = \cdots = x_n$. For elegant applications (suitable for the classroom) of this result to elementary geometry, see [**2**].

One of the simplest proofs of (1) consists in recognizing it to be merely a special case of Jensen's inequality [**3**]. This widely used result (e.g., probability theory [**4**]) states that if the graph of a real continuous function $f(x)$ is *concave down* then

$$\frac{\sum f(x_i)}{n} \leq f\left(\frac{\sum x_i}{n}\right), \tag{2}$$

with equality *iff* the x's are all equal. If the graph is concave up, the inequality is reversed. To obtain (1) we need only put $f(x) = \ln x$ and note that its graph is concave down. Very neat, but where did (2) come from? This note describes a particularly simple way of *seeing* its truth, which we hope may be of value in the classroom. Indeed, we believe it could even be used successfully in high schools.

We have given no formal definition of a graph being "concave down," and when presenting the following argument to young students we shall suppose that none *will* be given; what matters is that they know what one looks like. With more mature students we may define the graph of f to be "concave down" if the region $\{(x, y)\colon\ y \leq f(x)\}$ below the graph is convex. This is not one of the standard definitions, but it is a visually compelling inference from any other reasonable definition.

Consider a set of n point particles in the plane, of equal mass and with position vectors $\mathbf{r}_i$. The center of mass therefore has position vector

$$\mathbf{c} = \frac{1}{n}\sum \mathbf{r}_i,$$

from which it follows easily that

$$\sum (\mathbf{r}_i - \mathbf{c}) = \mathbf{0}.$$

In other words (see FIGURE 1), *the vectors from c to the particles cancel.*

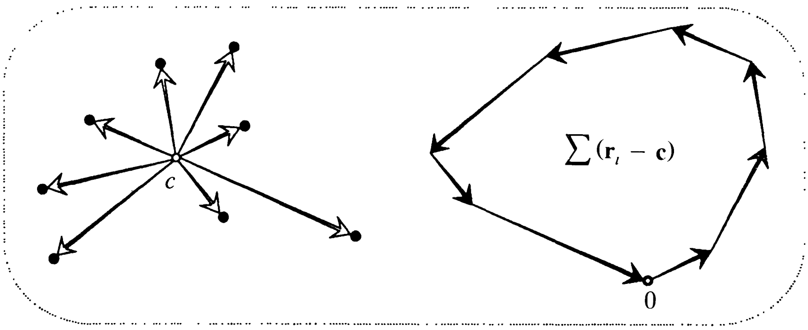


Figure 1

Imagining pegs sticking out of the plane at the locations of the particles, stretch a rubber band so as to enclose all the pegs. When released, the rubber band will contract into the dashed polygon H of FIGURE 2. This is the "convex hull" of the set of particles. The key point is this: *c must lie in the shaded interior of H*. For if p is outside this set, we see that the vectors from p to the particles cannot possibly cancel, as they must do for c. More formally, we take it as visually evident that through any exterior point p we may draw a line L such that H and its shaded interior lie entirely on one side of L. [Alternatively, this property may be taken as a (non-standard) *definition* of a convexity for a closed planar set.] The impossibility of the vectors cancelling now follows from their lying entirely on this side of L, for they all must have positive components in the direction of the normal vector $\mathbf{n}$. Except when the particles are collinear (in which case H collapses to a line-segment), the same reasoning forbids c from lying *on* H.

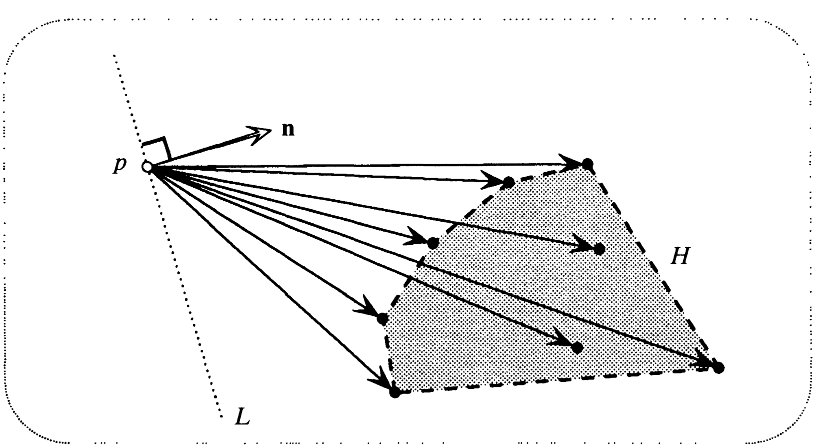


Figure 2

Next, suppose that the particles are distributed along a convex curve K. See FIGURE 3. The shaded interior of H now lies entirely on the concave side of K, and consequently so too must c. Furthermore, we see that c can only lie on K in the degenerate case that all the particles coalesce. Finally, take K to be the graph of a function $f(x)$. If this graph is *concave down* [*up*], then c lies *below* [*above*] K. Thus, with the particles located at $(x_i, f[x_i])$, we conclude that if the graph is

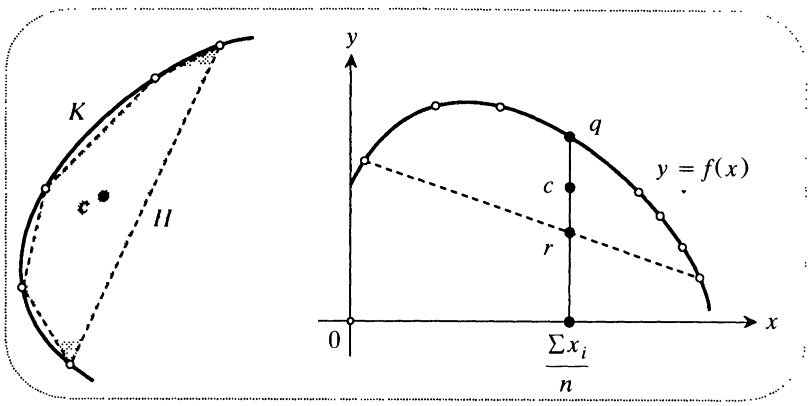


Figure 3

concave down,

$$\frac{\sum f(x_i)}{n} = \textit{height of } c \leq \textit{height of } q = f\left(\frac{\sum x_i}{n}\right),$$

with equality *iff* the x's are all equal. If the graph is concave up, the inequality is simply reversed.

As a bonus, observe that c must also lie on or above the dashed chord connecting the two end particles. Thus if $y = g(x)$ is the equation of this chord, we obtain

$$g\left(\frac{\sum x_i}{n}\right) = \textit{height of } r \leq \textit{height of } c = \frac{\sum f(x_i)}{n}.$$

I do not know if this result has a name.

We note that the above ideas can be generalized in at least two directions:

(1) The positive masses m_i of the particles need not be equal for the argument to work. Thus, once again taking the graph to be concave down,

$$\frac{\sum m_i f(x_i)}{M} \leq f\left(\frac{\sum m_i x_i}{M}\right),$$

where M denotes the total mass. This is essentially the form that is used in probability theory, for we are free to interpret (m_i/M) as a probability distribution for x_i, yielding

$$\mathscr{E}[f(x)] \leq f(\mathscr{E}[x]),$$

where $\mathscr{E}$ stands for the expected value. Also, by allowing the number of particles to increase without limit, we may pass from a discrete probability distribution to a continuous one.

(2) The argument is equally applicable to a set of particles in three-dimensional space. Thus, taking these particles (of equal mass, say) to be distributed over a surface $z = f(x, y)$ that is concave down, we deduce that

$$\frac{\sum f(x_i, y_i)}{n} \leq f\left(\frac{\sum x_i}{n}, \frac{\sum y_i}{n}\right).$$

Of course this too may be generalized to unequal masses and be given a probabilistic interpretation.

I do not wish to claim that the above is more original than it really is. In particular, the argument associated with FIGURE 2 is very old; I merely rediscovered it. The first important application of this idea that I know of occurred in 1874 when F. Lucas used it (see **[5]**) to demonstrate a complex analogue of Rolle's theorem: *the critical points of a polynomial in the complex plane must all lie within the convex hull of its zeros*. This follows from FIGURE 2 by observing [Gauss, 1816] that if $P(z)$ is the factorized polynomial, the conjugate of the logarithmic derivative $[P'(z)/P(z)]$ is a weighted sum of vectors from z to the zeros.

Also, consideration of centers of mass is certainly not new in the context of Jensen's inequality, and thus it is hard to believe that so simple a line of thought can have escaped notice. Nevertheless, it would appear that in the literature (e.g., **[1]**, p. 71) the location of the center of mass is merely used as an *interpretation* of (2), rather than as the source of an explanation.

ACKNOWLEDGMENTS. The idea of this note arose from a conversation (several years ago) with my friend Dr. George Burnett-Stuart. I also thank Dr. John Kao for explaining to me the significance of Jensen's inequality in probability theory. Finally, I am grateful to the referee for helpful comments on the first draft.

REFERENCES

1. G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*, Cambridge University Press, 1952.
2. G. Pólya, *Mathematics and Plausible Reasoning*, vol. 1, Princeton University Press, 1954, pp. 137–141.
3. D. S. Mitrinović, *Elementary Inequalities*, P. Noordhoff Ltd., Netherlands, 1964, pp. 23–30.
4. W. Feller, *An Introduction to Probability Theory and Its Applications*, 3rd edition, Vol. 2, Wiley, 1967.
5. J. L. Walsh, *The Location of Critical Points*, Amer. Math. Soc. Colloquium Publications, Vol. XXXIV, 1950, pp. 5–7.

Mathematics Department
University of San Francisco
2130 Fulton Street
San Francisco, CA 94117-1080

The Fine Memorial Mathematics Hall, which will be erected at Princeton University at a cost of $400,000 in memory of the late Henry B. Fine, for many years a professor of mathematics and dean of science, will be started in the near future.

36(1929), 453

The Index of a Constrained Critical Point

Catherine Hassell and Elmer Rees

1. INTRODUCTION. This note deals with the problem of determining the type of a critical point arising in the method of Lagrange multipliers. This method is the usual one used to solve the following problem:

To find the critical points of a smooth function f defined on $M^n \subset \mathbb{R}^{n+m}$, a smooth submanifold given as the common zero-set of m smooth functions g_i: $\mathbb{R}^{n+m} \to \mathbb{R}$.

The method consists of introducing a vector $\underline{\lambda} = (\lambda_1, \lambda_2, \dots, \lambda_m)$ of 'undetermined multipliers', defining L to be $f + \underline{\lambda} \cdot g = f + \Sigma_{i=1}^m \lambda_i g_i$ and finding its critical points. The question of deciding the non-degeneracy and type of a critical point is usually disregarded in the text books or else dismissed as being too complicated. Our purpose is to show, on the contrary, that criteria can be stated and derived in a straightforward manner.

We compare the Hessian of f restricted to M with the bordered Hessian, that is, the Hessian of L regarded as a function of $n + 2m$ variables (including $\underline{\lambda}$). The two Hessians have the same nullity at corresponding critical points and when they are non-degenerate, they have the same signature.

2. LAGRANGE MULTIPLIERS AND THE BORDERED HESSIAN. Let $U \subset \mathbb{R}^{n+m}$ be an open subset and $\underline{g}$: $U \to \mathbb{R}^m$ be a C^1-function such that $D\underline{g}(\underline{a})$: $\mathbb{R}^{n+m} \to \mathbb{R}^m$ has rank m for every $\underline{a} \in M = \{\underline{x} \in U | \underline{g}(\underline{x}) = \underline{c}\}$. Hence, by the implicit function theorem [**F**, p. 117], M is a smooth n-dimensional manifold. We wish to determine the critical points of the function f_1: $M \to \mathbb{R}$ which is the restriction of a C^2-function f: $U \to \mathbb{R}$.

For $\underline{\lambda} \in \mathbb{R}^m$, we consider the Lagrangian

$$L = f + \underline{\lambda} \cdot (\underline{g} - \underline{c})$$

either as a function of $\underline{x} \in U$ or as a function of $(\underline{x}, \underline{\lambda}) \in U \times \mathbb{R}^m$. The critical points are obtained by solving the equations

$$\nabla L = 0 \quad \text{and} \quad \underline{g} = \underline{c}$$

or, equivalently

$$\nabla L = 0$$

regarding L as a function of $(\underline{x}, \underline{\lambda})$.

To determine the nature of a critical point $\underline{a}$ of f_1 one could study the Taylor series of f_1 at $\underline{a}$ in terms of local coordinates on M. Let $H_M f(\underline{a})$ be the Hessian form of f_1; it is the symmetric bilinear form on the tangent space $T_{\underline{a}}(M)$ which represents the quadratic terms in the Taylor expansion of f_1. If $x_1, \dots, x_n$ are local coordinates on M near $\underline{a}$, the entries of the matrix of $H_M f(\underline{a})$ are $(\partial^2 f / \partial x_i\, \partial x_j)$

evaluated at $\underline{a}$. If this matrix is non-singular, the form $H_M f(\underline{a})$ is called non-degenerate and f_1 is called a Morse function at $\underline{a}$. In this case the nature of the critical point is determined by the algebraic properties of $H_M f(\underline{a})$. The index of the critical point, that is the number of independent directions in which f_1 decreases, is determined by the signature of the form $H_M f(\underline{a})$. We will give practical methods for determining when $H_M f(\underline{a})$ is non-degenerate and for calculating its signature.

Let $\underline{g}$ be a C^2-function and let $HL(\underline{a}, \underline{\lambda})$ be the bordered Hessian of L at the critical point $(\underline{a}, \underline{\lambda})$ of L; that is, the Hessian of L regarded as a bilinear form on $T_{(\underline{a}, \underline{\lambda})}(U \times \mathbb{R}^m) \cong \mathbb{R}^{n+2m}$. If

$$\underline{g}^T = (g_1, g_2, \dots, g_m)$$

let $D\underline{g}^T = (\nabla g_1, \nabla g_2, \dots, \nabla g_m)$ denote the (transposed) Jacobian matrix of $\underline{g}$ at $\underline{a}$. Then the matrix of the bordered Hessian $HL(\underline{a}, \underline{\lambda})$ is the $(n + 2m)$ by $(n + 2m)$ symmetric matrix

$$\begin{bmatrix} Hf + \underline{\lambda} \cdot H\underline{g} & D\underline{g}^T \\ D\underline{g} & 0 \end{bmatrix}$$

where $\underline{\lambda}$ is evaluated from the equation

$$0 = \nabla L = \nabla f + \underline{\lambda} \cdot D\underline{g}$$

at $\underline{a}$.

3. THE MAIN RESULT. If a symmetric bilinear form on a real vector space is represented by the matrix H; then its nullity is the dimension of the kernel of H and its signature is $p - q$, where p and q denote the number of positive and negative eigenvalues of H respectively.

Theorem 1. *The nullity of $H_M f(\underline{a})$ equals the nullity of $HL(\underline{a}, \underline{\lambda})$.*

If $HL(\underline{a}, \underline{\lambda})$ (and hence $H_M f(\underline{a})$) is non-degenerate, then the signature of $H_M f(\underline{a})$ equals that of $HL(\underline{a}, \underline{\lambda})$.

This theorem follows from the purely algebraic Theorem 2, using Taylor's formula and the implicit function theorem [F]. When it is applied to critical points as above, it yields the following result.

Corollary. *The point $\underline{a} \in M$ is a critical point of f_1: $M \to \mathbb{R}$ if and only if $(\underline{a}, \underline{\lambda})$ is a critical point of L: $U \times \mathbb{R}^m \to \mathbb{R}$. In this case, $\underline{a}$ is non-degenerate if and only if $(\underline{a}, \underline{\lambda})$ is non-degenerate and the index $I(f_1, \underline{a})$ of f_1 at $\underline{a}$ is related to the index $I(L, \underline{a}, \underline{\lambda})$ of L at $(\underline{a}, \underline{\lambda})$ by*

$$I(f_1, \underline{a}) + m = I(L, \underline{a}, \underline{\lambda}).$$

So, for example, $\underline{a}$ is a local minimum of f_1 if $(\underline{a}, \underline{\lambda})$ is a non-degenerate critical point of L of index m.

Similarly, $\underline{a}$ is a local maximum of f_1 if $(\underline{a}, \underline{\lambda})$ is a non-degenerate critical point of L of index $n + m$.

Theorem 2. *Let $C = \begin{bmatrix} A & B^T \\ B & 0 \end{bmatrix}$ be the symmetric real matrix consisting of the $(n + m) \times (n + m)$ symmetric matrix A, the $m \times (n + m)$ matrix B of rank m and the zero*

$m \times m$ matrix 0. The symmetric bilinear form induced on $\operatorname{Ker} B$ *by A is denoted b. Then the bilinear form on $\mathbb{R}^{n+2m}$ defined by C is isomorphic to $b \oplus H$ where H is the $2m$-dimensional hyperbolic form* $\begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$.

The proof that we give for this theorem is considerably simpler than our original one and is based on a proof provided for us by Dr. A. A. Ranicki.

First, we give proofs of some facts from linear algebra that we need.

Fact 1 (Fredholm alternative) [**HK**, p. 103]. Let P^T: $\mathbb{R}^k \to \mathbb{R}^l$ be the transpose of the matrix P: $\mathbb{R}^l \to \mathbb{R}^k$, then

$$(\operatorname{Ker} P)^{\perp} = \operatorname{Im} P^T.$$

Proof: Let r denote rank P. Then $\dim \operatorname{Ker} P = l - r$ hence $\dim(\operatorname{Ker} P)^{\perp} = r$. Also $\dim \operatorname{Im} P^T = r$. It is therefore enough to show that $\operatorname{Im} P^T \subset (\operatorname{Ker} P)^{\perp}$ i.e.

$$\operatorname{Im} P^T \perp \operatorname{Ker} P.$$

Suppose $\underline{x} \in \mathbb{R}^k$ and $\underline{z} \in \operatorname{Ker} P$ then

$$\underline{z} \cdot P^T\underline{x} = \underline{z}^T P^T \underline{x} = 0 \quad \text{since } P\underline{z} = 0.$$

Let b be a bilinear form on the real finite dimensional space V, the annihilator of a subspace $U \subset V$ is $U^{\perp} = \{\underline{x} \in V | b(\underline{x}, \underline{u}) = 0 \ \forall \underline{u} \in U\}$.

Fact 2. Let b be a non-degenerate symmetric bilinear form on V of dimension $2m$ and let $W \subset V$ have dimension m and $W \subset W^{\perp}$. Then b is represented by the matrix $\begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$.

Proof: Choose $\underline{w} \neq 0$ in W and $\underline{v}$ such that $b(\underline{w}, \underline{v}) = 1$. Let $\underline{u} = \underline{v} - b(\underline{v}, \underline{v})\underline{w}/2$, then $b(\underline{u}, \underline{u}) = 0$ and $\{\underline{u}, \underline{w}\}$ is the required basis in the case $m = 1$. When $m > 1$, let $U = \operatorname{Span}\{\underline{u}, \underline{w}\}$ and consider $U^{\perp}$, this contains a subspace that is self-annihilating and of dimension $m - 1$. The result follows by induction.

We also make use of the principal axis theorem.

Fact 3 [**HK**, p. 266]. If b is a symmetric bilinear form on an n-dimensional real inner product space then there is an orthonormal basis $\{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$ such that $b(\underline{e}_i, \underline{e}_j) = \delta_{ij} a_i$ for some $a_i \in \mathbb{R}$.

Proof of Theorem 2: If W denotes the m-dimensional subspace

$$\left\{ \begin{pmatrix} 0 \\ - \\ \underline{y} \end{pmatrix} : \underline{y} \in \mathbb{R}^m \right\} \subset \mathbb{R}^{n+2m},$$

then by Fact 1 applied to B, there is a canonical orthogonal decomposition

$$\mathbb{R}^{n+2m} \cong \operatorname{Ker} B \oplus \operatorname{Im} B^T \oplus W.$$

By Fact 3, one can choose an orthonormal basis

$$\{\underline{e}_1, \ldots, \underline{e}_n\} \textit{ for } \operatorname{Ker} B$$

such that $b(\underline{e}_i, \underline{e}_i) = a_i$ and $b(\underline{e}_i, \underline{e}_j) = 0$ for $i \neq j$. Then for $1 \leqslant i \leqslant n$, $\underline{e}_i$ is a vector whose component in W is zero. Since $\underline{e}_i \in \operatorname{Ker} B$ one has $C\underline{e}_i \in W^{\perp}$ and hence $C\underline{e}_i = \underline{k}_i + B^T \underline{f}_i$ where $\underline{k}_i \in \operatorname{Ker} B$ and $\underline{f}_i \in \mathbb{R}^m \cong W$ is unique because B^T

is one-to-one. Moreover, $\underline{k}_i = \underline{a}_i\underline{e}_i$ because $\underline{e}_j^T C \underline{e}_i = \delta_{ij} a_i$. Hence,

$$\begin{aligned} C\underline{e}_i &= a_i\underline{e}_i + B^T \underline{f}_i \\ &= a_i\underline{e}_i + C\underline{f}_i \end{aligned}$$

Define $K = \operatorname{Span}\{\underline{e}_i - \underline{f}_i\colon 1 \leqslant i \leqslant n\}$.
The following steps will prove Theorem 2.

Step 1. K and $\operatorname{Im} B^T \oplus W$ are orthogonal with respect to C.

Step 2. The form defined by C on K is isomorphic to b.

Step 3. The form defined by C on $\operatorname{Im} B^T \oplus W$ is hyperbolic.

Proof of Step 1: Since $C(\underline{e}_i - \underline{f}_i) = a_i\underline{e}_i \in \operatorname{Ker} B$, one has that $C(K) \subset \operatorname{Ker} B$ and $\operatorname{Ker} B$ is orthogonal to $\operatorname{Im} B^T \oplus W$.

Proof of Step 2: Since $(\underline{e}_j - \underline{f}_j)^T C(\underline{e}_i - \underline{f}_i) = a_i \delta_{ij}$, one has that $C|K$ is isomorphic to b.

Proof of Step 3: By choosing a basis for the image of B^T, one can take the matrix of C to have the following form

$$\begin{bmatrix} A_1 & A_2^T & 0 \\ A_2 & A_3 & I_m \\ 0 & I_m & 0 \end{bmatrix}.$$

Hence the matrix of $C|\operatorname{Im} B^T \oplus W$ has the form

$$\begin{bmatrix} A_3 & I_m \\ I_m & 0 \end{bmatrix}$$

and so is equivalent to a hyperbolic form by Fact 2, since W is a self-annihilating subspace of dimension m.

4. COMPARISON WITH CLASSICAL CRITERIA. In the literature there are criteria for deciding when a critical point is a local maximum or minimum, for example **[H]** or **[G]**. Here we show how these criteria are related to our result.

Criterion 1. Let $C = \begin{bmatrix} A & B^T \\ B & 0 \end{bmatrix}$ be as in Theorem 2 and assume that the last $m \times m$ submatrix of B is non-singular, then the form induced by A on $\operatorname{Ker} B$ is positive definite if the determinants Δ_i for $0 \leqslant i \leqslant n$ have sign $(-1)^m$ where $\Delta_i = \det C_i$ and C_i is obtained from C by deleting its first i rows and columns.

Proof: Write $C_n = \begin{bmatrix} A_n & B_n^T \\ B_n & 0 \end{bmatrix}$. Then $\Delta_n = \det C_n = (-1)^m (\det B_n)^2$, so sign $\Delta_n = (-1)^m$ since B_n is non-singular. By Fact 2, C_n is hyperbolic and so has index m.

The proof is completed by using induction based on the following:

Lemma. *Let H be a non-singular symmetric real matrix and H_1 be obtained from H by deleting one row and the corresponding column. If H_1 is also non-singular and*

index H is the number of negative eigenvalues of H then

$$\text{index } H = \begin{cases} \text{index } H_1 \\ \text{index } H_1 + 1 \end{cases}$$

depending on whether $\det H$ *and* $\det H_1$ *have the same or the opposite sign.*

Proof: Let M and M_1 be maximal negative definite subspaces for H and H_1 respectively.

Recall that the dimension of a maximal negative definite subspace is unique.

Clearly, $\dim M_1 \leqslant \dim M \leqslant \dim M_1 + 1$.

Also $\operatorname{sign}\det H = (-1)^{\dim M}$ and $\operatorname{sign}\det H_1 = (-1)^{\dim M_1}$.

Hence $\det H$ and $\det H_1$ have the same sign $\Leftrightarrow \dim M = \dim M_1$ as required.

Another criterion discovered in the 19th century is the following (see **[H]** for the historical references).

Criterion 2. Let $\begin{bmatrix} A & B^T \\ B & 0 \end{bmatrix}$ be as in Theorem 2. Then the form induced by A on $\operatorname{Ker} B$ is positive definite if and only if the roots of

$$\det\begin{bmatrix} A - tI & B^T \\ B & 0 \end{bmatrix} = 0$$

are all positive.

Note that the above equation is of degree n.

The stronger result that the roots of the above equation are the eigenvalues of the form A restricted to $\operatorname{Ker} B$ with the same multiplicities is an immediate consequence of Theorem 2 applied to the matrix

$$\begin{bmatrix} A - tI & B^T \\ B & 0 \end{bmatrix}$$

when t is a root of the above equation.

5. EXAMPLES

1. To find the critical points of $f(x, y, z) = x^3 + y^3 + z^3$ on the surface $x^{-1} + y^{-1} + z^{-1} = 1$. (This example is taken from **[G**, p. 94]).

Let $L = x^3 + y^3 + z^3 + \lambda(x^{-1} + y^{-1} + z^{-1} - 1)$ then $(\partial L/\partial x) = 3x^2 - \lambda x^{-2}$ etc. and the bordered Hessian is

$$\begin{bmatrix} 6x + 2\lambda x^{-3} & 0 & 0 & -x^{-2} \\ 0 & 6y + 2\lambda y^{-3} & 0 & -y^{-2} \\ 0 & 0 & 6z + 2\lambda z^{-3} & -z^{-2} \\ -x^{-2} & -y^{-2} & -z^{-2} & 0 \end{bmatrix}.$$

The critical points are given by

$$x^4 = y^4 = z^4 = \lambda/3 \text{ and } x^{-1} + y^{-1} + z^{-1} = 1.$$

These are $x = y = z = 3$, $\lambda = 243$; $x = y = 1$, $z = -1$, $\lambda = 3$ and two other solutions symmetrical with the latter.

In the first case the Hessian is

$$\begin{pmatrix} 36 & 0 & 0 & -9^{-1} \\ 0 & 36 & 0 & -9^{-1} \\ 0 & 0 & 36 & -9^{-1} \\ -9^{-1} & -9^{-1} & -9^{-1} & 0 \end{pmatrix}$$

which is non-degenerate and has signature 2, so the critical point has index 0; that is, it is a non-degenerate minimum.

In the second case the Hessian is

$$\begin{pmatrix} 12 & 0 & 0 & -1 \\ 0 & 12 & 0 & -1 \\ 0 & 0 & -12 & -1 \\ -1 & -1 & -1 & 0 \end{pmatrix}$$

which is non-degenerate and has signature 0. So this critical point (and the other two symmetrical with it) has index 1; that is, it is a saddle point.

2. Consider the quadratic form $\underline{x}^T A \underline{x}$ on the sphere $\underline{x}^T \underline{x} = 1$ in $\mathbb{R}^n$. Critical points $\underline{x}$ are given by

$$A\underline{x} - \lambda \underline{x} = 0$$

i.e. by an eigenvector $\underline{x}$ with eigenvalue λ. The critical point is non-degenerate if $\begin{bmatrix} A - \lambda I & \underline{x} \\ \underline{x}^T & 0 \end{bmatrix}$ is non-singular and this is true if the eigenvalue has multiplicity 1. If the eigenvalue has multiplicity $r > 1$, let $\underline{x}_1, \ldots, \underline{x}_r$ be a basis for the eigenspace, then

$$\begin{bmatrix} A - \lambda I & \underline{x}_1 & \cdots & \underline{x}_r \\ \underline{x}_1^T & & & \\ \vdots & & \mathbf{0} & \\ \underline{x}_r^T & & & \end{bmatrix}$$

is non-singular. The corresponding critical submanifold is a great sphere of dimension $r - 1$ and is non-degenerate in Bott's sense [**B**]. We recall this concept briefly. Let S be a connected critical submanifold for a function f; it is called non-degenerate if for every $\underline{x} \in S$, the Hessian is non-degenerate normal to S, i.e. the Hessian is zero on $T_{\underline{x}}S$ and the induced form on $T_{\underline{x}}M/T_{\underline{x}}S$ is non-degenerate. If $M^n \subset \mathbb{R}^{n+m}$ is defined by $\underline{g} = \underline{c}$, then the bordered Hessian is

$$HL(\underline{a}, \underline{\lambda}) = \begin{bmatrix} Hf + \underline{\lambda} \cdot H\underline{g} & D\underline{g}^T \\ D\underline{g} & 0 \end{bmatrix}.$$

If $\{\underline{e}_1, \ldots, \underline{e}_l\}$ is a basis for $T_{\underline{a}}S$, $\underline{e}_i \in \mathbb{R}^{n+m}$, then S is non-degenerate at $\underline{a}$ if

$$\begin{bmatrix} Hf + \underline{\lambda} \cdot H\underline{g} & D\underline{g}^T & E^T \\ D\underline{g} & 0 & 0 \\ E & 0 & 0 \end{bmatrix}$$

is non-singular, where E^T is the matrix $(\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_l)$. The signature of this enlarged bordered Hessian determines the index of the critical submanifold in the same way as our main result deals with non-degenerate critical points.

REFERENCES

Early references that discuss the general problem are listed in **[H**, chapter VI]. Some of the more recent references for the problem are **[M2]**, **[D]**, **[G]**, **[S2]**, **[M1]**. The paper **[S1]** considers the case of a single constraint equation and includes the results of this note in that case.

[B] R. Bott, Non-degenerate critical manifolds, *Ann. of Math.* (2) 60 (1954) 248–261.
[D] G. Debreu, Definite and semidefinite quadratic form, *Econometrica* 20 (1952) 295–300.
[F] W. H. Fleming, *Functions of Several Variables*, Addison Wesley, 1965.
[G] R. P. Gillespie, *Partial Differentiation*, Oliver & Boyd, 1954.
[H] H. Hancock, *Theorem of Maxima and Minima*, Ginn & Co., 1917, Dover, 1960.
[HK] K. Hoffman and R. Kunze, *Linear Algebra*, Prentice Hall, 1961.
[M1] J. H. Maddocks, Restricted quadratic forms, inertia theorems and the Schur complement, *Linear Alg. Appl.* 108 (1988) 1–36.
[M2] H. B. Mann, Quadratic forms with linear constraints, *Amer. Math. Monthly* 50 (1943) 430–433.
[S1] T. Sakkalis, The computation of the index of a Morse function at a critical point, *Internat. J. Math & Math. Sci.* 11 (1988) 721–726.
[S2] D. Spring, On the second derivative test for constrained local extrema, *Amer. Math. Monthly* 92 (1985) 631–643.

Department of Mathematics and Statistics
The University of Edinburgh
Edinburgh EH9 3JZ, Scotland

A Characterization of Euclidean Spaces

In connection with the article "A Characterization of Inner Product Spaces" by Neil Falkner (this *Monthly* 100(1993), 246–249) it might be worth noting that inner product spaces over the reals are characterized by the validity of the Converse Theorem of Pythagoras. The latter, namely that the smaller sides of a triangle which fulfills the famous Pythagorean relation $a^2 + b^2 = c^2$ are orthogonal, is often assumed without proof as for instance in the argument about the legendary rope-stretchers of Ancient Egypt, who are said to have used a triangle with sides 3, 4, 5 to construct a right angle.

In the notions of an inner product space we have $\|x + y\|^2 = \|x\|^2 + 2\,\mathrm{re}(x, y) + \|y\|^2$. So the Theorem of Pythagoras and its converse are obvious in the case of a real inner product space. However, in any complex inner product space (with the exception of the trivial space $\{0\}$, which is no real complex space anyway) we may take $x \neq 0$ and $y := \mathrm{i}\,x$ such that $(x, y) = \mathrm{i}\|x\|^2 \neq 0$, but still $\|x + y\|^2 = \|x\|^2 + \|y\|^2$ holds true.

The fact that in Euclid's *Elements* the Theorem of Pythagoras (I.47) is followed by the Converse Theorem of Pythagoras (I.48) and its proof is another justification for calling inner product spaces over the reals Euclidean spaces.

Andreas M. Hinz
Mathematisches Institut
Universität München
Theresienstraße 39
D-80333 München
andreas.hinz@mathematik.uni-muenchen.dbp.de

On Some Irrational Decimal Fractions

Norbert Hegyvári

It is known that the decimal fraction

$$\alpha = 0.235711131719\ldots$$

is irrational, where the sequence of digits is formed by the primes in ascending order. In [**1**, Th. 138] there are two different proofs for this statement. The first uses a special case of the Dirichlet's theorem, namely: any arithmetical progression of the form $10^{s+1}k + 1$ $(k = 1, 2, \cdots)$ contains primes. In the second proof it is assumed that there is a prime between N and $10N$ for every $N > 0$, which is the special case of the Bertrand's Postulate. Similar proofs are found in [**2**].

In this article we will give a direct proof for this statement. We prove even more.

Theorem. *Let $1 \leqslant a_1 < a_2 < \ldots$ be a sequence of integers for which $\sum_{i=1}^{\infty} 1/a_i = \infty$. Then the decimal fraction $\alpha = 0 \cdot (a_1)(a_2)\ldots(a_n)\ldots$ is irrational.*

Since $\sum_{i=1}^{\infty} 1/p_i = \infty$, where $p_1 < p_2 < \ldots$ is the sequence of primes, we immediately get the original version of the statement.

Definition. Let B be a block of digits $b_1 b_2 \ldots b_s$ with $s \geq 1$ and $0 \leq b_i \leq 9$ for $i = 1, 2, \ldots, s$. Let n be a positive integer $\sum_{i=0}^{k} c_i 10^{k-i}$ with $c_0 \neq 0$. The integer n is said to contain the block of digits B if for some $j \geq 0$ we have $c_{i+j} = b_i$ for every $i = 1, 2, \ldots, s$. For example, the integer 1402857 contains the blocks 14 and 0285 (among others), but not the blocks 014 or 582.

Lemma. *If $X = X(b_1, b_2, \ldots, b_s)$ denotes the sequence of positive integers not containing the block of digits $b_1 b_2 \ldots b_s$, then $\sum_{n \in X}^{\infty} 1/n$ is convergent.*

We mention that the Lemma is a generalization of a well-known exercise (see [**1**, Th 144]).

Proof of the Lemma: Let $s_n = 1/x_1 + 1/x_2 + \ldots 1/x_n$ and let t be an integer for which $x_{t-1} < 10^s \leq x_t$. Then we have

$$s_n < 1/x_1 + 1/x_2 + \ldots + 1/x_t + 10^{-s}(1/[x_{t+1}/10^s] + \ldots + 1/[x_n/10^s]).$$

We note that if $t < i \leq n$, then $[x_i/10^s]$ is a member of X, say x_j. Also, since the block $b_1 b_2 \ldots b_s$ appears in at least one of 10^s consecutive integers, it follows that for any fixed x_j there are at most $10^s - 1$ values of x_j such that $[x_i/10^s] = x_j$, and we have

$$s_n < \sum_{i=1}^{t} 1/x_i + (10^s - 1)10^{-s} s_n \quad \text{or} \quad s_n < 10^s \cdot \sum_{i=1}^{t} x_i,$$

which proves the lemma.

Proof of the Theorem: Assume that α is a rational number. Thus α is a periodic decimal, with a block of digits, say $b_1b_2\dots b_s$, repeating endlessly perhaps after an initial first block. If B is a block of 1's, define $c_1c_2\dots c_{2s}$ to be a block of 2's of length $2s$; otherwise define $c_1c_2\dots c_{2s}$ to be a block of 1's of length $2s$. Now define $Y = Y(c_1, c_2, \dots, c_{2s})$ as the sequence of natural numbers not containing the block of digits $c_1c_2\dots c_{2s}$. If we write

$$\sum_{i=1}^{\infty} 1/a_i = \sum_{a\in Y} 1/a + \sum_{a\notin Y} 1/a,$$

then by the Lemma the first sum on the right side converges, and hence the second sum diverges. This implies that there are infinitely many a_i that contain the block of digits $c_1c_2\dots c_{2s}$. This in turn implies that B cannot be a repeating block of digits in α. This contradiction establishes the Theorem.

ACKNOWLEDGMENT. The author would like to thank the referee for a number of suggestions and for detecting some flaws in our original version.

REFERENCES

1. Hardy–Wright, *An Introduction to the Theory of Numbers*, fifth edition, Oxford, Clarendon Press, 1979.
2. G. Pólya–G. Szegö, *Problems and Theorems in Analysis II.*, Springer-Verlag, 1976, (exercise 257.)

Department of Math. L. Eötvös Univ. and
Math. Inst. of the Hung. Acad. of Sci.
Budapest, Pf 127, H-1364
Hungary

Professor Florian Cajori died suddenly of pneumonia on August 14, 1930, at his home in Berkeley, California. He was a charter member of the Mathematical Association of America and was one of an original group of four (later enlarged to twelve) representatives of mid-western universities and colleges who made possible the re-establishment of the American Mathematical Monthly on a sound financial basis. A detailed account of his historical researches will be published in the *Monthly* in due course.

37(1930), 392

NOTES

Edited by: **John Duncan**

The Symmetry Principle for Möbius Transformations

Louis Brickman

With precise definitions to come below, the symmetry principle is the following.

Theorem. *Let E be a circle or extended line. Let T be a Möbius transformation. Let z and z^* be symmetric points with respect to E. Then $T(z)$ and $T(z^*)$ are symmetric with respect to $T(E)$ (which is also a circle or extended line).*

Can the discussion be both rigorous and intuitively satisfying? The key is that the theorem is more about "conjugate Möbius transformations" than ordinary Möbius transformations. Indeed, the theorem holds for either type of transformation, whereas the symmetry concept involves only the former. To prepare the proof we need only set down the composition relationships between the two types (Lemma 1), and then show that each circle or extended line determines a unique and very special conjugate Möbius transformation (Lemma 2).

Many of the standard proofs establish the conclusion separately for special transformations such as translations, inversions, and dilations. The results are then combined in a composition argument. Another well known approach depends upon the concept of cross ratio. The method here seems simplest.

Preliminary Definitions. The complex plane and extended complex plane are denoted by $\mathbf{C}$ and $\hat{\mathbf{C}}$, respectively ($\hat{\mathbf{C}} = \mathbf{C} \cup \{\infty\}$). A *Möbius transformation* is a map T: $\hat{\mathbf{C}} \to \hat{C}$ defined by

$$T(z) = \frac{az+b}{cz+d} \qquad (a, b, c, d, \in \mathbf{C};\ ad - bc \neq 0).$$

The formula is extended by continuity for $z = \infty$ and, if $c \neq 0$, for $z = -d/c$. With each such T we associate the *conjugate Möbius transformation* $\overline{T}$: $\hat{\mathbf{C}} \to \hat{\mathbf{C}}$ defined by

$$\overline{T}(z) = \overline{T(z)} \qquad (\overline{\infty} = \infty).$$

Finally, we let $\mathscr{M}$ be the set (actually "group") of all Möbius transformations and $\overline{\mathscr{M}}$ be the set of all conjugate Möbius transformations.

We remark (without proof) that our first lemma is equivalent to the statement that $\mathscr{M} \cup \overline{\mathscr{M}}$ is a group, and $\mathscr{M}$ and $\overline{\mathscr{M}}$ are the cosets of the normal subgroup $\mathscr{M}$.

Lemma 1. *Let $S, T \in \mathscr{M}$. Then*

$$(1)\ T \circ S \in \mathscr{M}, \qquad (2)\ T \circ \overline{S} \in \overline{\mathscr{M}}, \qquad (3)\ \overline{T} \circ S \in \overline{\mathscr{M}}, \qquad (4)\ \overline{T} \circ \overline{S} \in \mathscr{M}.$$

Proof: Conclusion (1) is standard. Then (3) follows immediately because $\overline{T} \circ S = \overline{T \circ S}$. Once (2) is proved, (4) follows from the fact that $\overline{T} \circ \overline{S} = T \circ \overline{\overline{S}}$. Thus we need only prove (2). With T as described above,

$$(T \circ \overline{S})(z) = T(\overline{S}(z)) = \frac{a\overline{S}(z) + b}{c\overline{S}(z) + d} = \left[\frac{\overline{a}S(z) + \overline{b}}{\overline{c}S(z) + \overline{d}}\right]^{-}.$$

Conclusion (2) now follows from (1).

Lemma 2. *For each circle or extended line E, there is a unique $\overline{T} \in \overline{\mathscr{M}}$ such that*

$$E = \left\{z \in \hat{\mathbf{C}}: \overline{T}(z) = z\right\}.$$

(E is exactly the set of fixed points of $\overline{T}$.) This $\overline{T}$ is an involution of $\hat{\mathbf{C}}$; that is, $\overline{T} \circ \overline{T}$ is the identity.

Proof: A circle described by $|z - a| = r(r > 0)$ is equivalently described by

$$z = \overline{T}(z) = \frac{r^2}{\overline{z - a}} + a.$$

A line $\{a + bt: t \in \mathbf{R}\}(b \neq 0)$ has the equation

$$\frac{z - a}{b} = \left(\frac{z - a}{b}\right)^{-}, \quad \text{or} \quad z = \overline{T}(z) = \frac{b}{\overline{b}}(\overline{z - a}) + a.$$

Since $\overline{T}(\infty) = \infty$, the extended line $\{a + bt: t \in \mathbf{R}\} \cup \{\infty\}$ is exactly the set of fixed points of $\overline{T}$.

For uniqueness suppose $\overline{T}_1(z) = z = \overline{T}_2(z)$ for all z on a circle or extended line. Then $T_1(z) = T_2(z)$ for more than 2 values of z. Hence $T_1 = T_2$ and $\overline{T}_1 = \overline{T}_2$. (The uniqueness of $\overline{T}$ for an extended line may be surprising in view of the fact that a and b are not uniquely determined by the extended line.)

For the involution proof we note that $\overline{T} \circ \overline{T} \in \mathscr{M}$ (Lemma 1, part (4)) and has all the points of E as fixed points.

Definition. The transformation $\overline{T}$ described in LEMMA 2 is called *reflection in E*, and will be denoted by ρ_E. If confusion seems unlikely, $\rho_E(z)$ is denoted simply by $z^*(z \in \hat{\mathbf{C}})$. Also, z and z^* are said to be *symmetric with respect to E.*

Now that reflection is solidly defined it is easy to prove the theorem. With obvious changes the proof applies equally well to conjugate Möbius transformations.

Proof of Symmetry Principle: In precise terms we must show that

$$\rho_{T(E)}(T(z)) = T(\rho_E(z)) \qquad (z \in \hat{\mathbf{C}}),$$

or

$$\rho_{T(E)} \circ T = T \circ \rho_E.$$

But both sides of the last equation belong to $\overline{\mathscr{M}}$ (Lemma 1, parts (2) and (3)), and they agree everywhere on E. Therefore we are finished.

Department of Mathematics and Statistics
State University of New York at Albany
Albany, New York 12222

A Short Proof for Romberg Integration

T. von Petersdorff

The Romberg extrapolation method for numerical integration is discussed in most numerical analysis textbooks. We give a short proof for the convergence rates of the Romberg extrapolations without using the Euler-Maclaurin formula.

The Romberg method starts with the sequence of values T_N of the composite trapezoid rule with $N = 1, 2, 4, 8, \dots$ subintervals which converges to the exact integral with a rate of $O(N^{-2})$. By using linear combinations of the values T_N new sequences $T_{N,1}, T_{N,2}, \dots$ are constructed which converge to the exact integral with the rates of $O(N^{-4}), O(N^{-6}), \dots$ for $N \to \infty$. We will see that the gain of two powers of N with each extrapolation step is due to the symmetry of the trapezoid rule.

The classical proof of the Romberg method on an interval uses the Euler-Maclaurin formula to derive an asymptotic expansion of the error of the composite trapezoid rule (e.g., **[2]**). The convergence rate of the Romberg extrapolations then follows from this expansion and the fact that it contains only even powers of N.

The proof of the Euler-Maclaurin formula is elementary. But the proof is based on certain recursion properties of the Bernoulli polynomials and it is not intuitively obvious what it is that makes the Romberg method work.

The convergence properties of the Romberg method can be understood by using homogeneity and symmetry principles, see e.g. **[1]** and the references given there. Here we want to give a simple proof which only uses these two basic principles (and Taylor's theorem). We will only derive the convergence rates of the extrapolated values based on the sequence of $1, 2, 4, 8, \dots$ subintervals. We do not obtain a general asymptotic expansion or formulae for the constants in the estimates. For results of this type see **[2]**, **[1]** and the references given there.

THE ROMBERG INTEGRATION METHOD. Let f be a continuous function on the interval $[a, b]$, and let $I(f) = \int_a^b f(x)\,dx$. The *trapezoid rule* on $[a, b]$ is defined by

$$T^{[a,b]}(f) = \tfrac{1}{2}(b-a)(f(a) + f(b))$$

and the *composite trapezoid rule* with N subintervals on $[a, b]$ is given by

$$T_N^{[a,b]}(f) = \sum_{k=1}^{N} T^{[x_{k-1},x_k]}(f) = \frac{1}{2}\frac{b-a}{N}\left(f(a) + f(b) + 2\sum_{k=1}^{N-1} f(x_k)\right)$$

where $x_k = a + k(b-a)/N$, $k = 0, \dots, N$. The *Romberg extrapolations* are defined recursively by

$$T_{k,0}(f) = T_k^{[a,b]}(f), \qquad T_{2k,m+1}(f) = \frac{2^{2m+2}T_{2k,m}(f) - T_{k,m}(f)}{2^{2m+2} - 1}$$

for integers $k \geq 1$, $m \geq 0$. The convergence is given by the following theorem:

Theorem 1. *Let f be $2m+2$ times continuously differentiable on $[a, b]$. Let $N = 2^m n$ with positive integers m, n. Then*

$$|T_{N,m}(f) - I(f)| \leq C_m(b-a)^{2m+3} \max_{\xi\in[a,b]} |f^{(2m+2)}(\xi)| n^{-(2m+2)} \tag{1}$$

Here the constant C_m is independent of f, a, b, N.

THE PROOF. We consider an integration rule on $[-1,1]$ of the form

$$A(f) = \sum_{j=1}^{J} f(\xi_j) w_j \tag{2}$$

with certain nodes $\xi_j \in \mathbb{R}$ and weights $w_j \in \mathbb{R}$, $j = 1, \ldots, J$. The corresponding rule for the interval $[a,b]$ is given by $A^{[a,b]}(f) = \frac{1}{2}(b-a)A(\tilde{f})$ where $\tilde{f}(x) = f(((a+b)+(b-a)x)/2)$. We will use the following theorem which is a standard result in numerical analysis textbooks and follows from Taylor's theorem.

Theorem 2. *Assume the integration rule* (2) *is exact for all polynomials of degree less than or equal to r, let f be $r+1$ times continuously differentiable. Then the composite rule $A_N^{[a,b]}(f) = \sum_{k=1}^{N} A^{[x_{k-1},x_k]}(f)$ satisfies for all positive integers N*

$$\left|A_N^{[a,b]}(f) - I(f)\right| \leq C(b-a)^{r+2} \max_{\xi \in [a,b]} \left|f^{(r+1)}(\xi)\right| N^{-(r+1)}$$

where the constant C is independent from f, a, b, N.

We now make the following assumption about $A(f)$:

Assumption 1. *Let the integration rule $A(f)$ on $[-1,1]$ be symmetric with respect to 0, i.e., $A(\tilde{f}) = A(f)$ where $\tilde{f}(x) = f(-x)$, for all continuous f. Furthermore, let the rule $A(f)$ be exact for all polynomials of degree less than or equal to q with some even number q.*

Then we have

Proposition 1. *The rule $A(f)$ is also exact for all polynomials of degree $q+1$.*

Proof: The function x^{q+1} is odd, hence $A(x^{q+1}) = 0$ and $\int_{-1}^{1} x^{q+1}\,dx = 0$.

Now we consider the composite rule $A_2(f(x)) = \frac{1}{2}A(f((x-1)/2)) + \frac{1}{2}A(f((x+1)/2))$ with two subintervals on $[-1,1]$ and denote the quadrature errors by $E(f) = A(f) - I(f)$, $E_2(f) = A_2(f) - I(f)$. Then

$$E_2(x^{q+2}) = \frac{1}{2}E\left(\left(\frac{x-1}{2}\right)^{q+2}\right) + \frac{1}{2}E\left(\left(\frac{x+1}{2}\right)^{q+2}\right) = 2^{-(q+2)}E(x^{q+2}) \tag{3}$$

by expanding the powers and using Proposition 1. Therefore we can integrate x^{q+2} exactly with the rule

$$\tilde{A}(f) = \frac{2^{q+2}A_2(f) - A(f)}{2^{q+2}-1} \tag{4}$$

Hence this construction implies:

Proposition 2. *The rule $\tilde{A}(f)$ is symmetric and exact for all polynomials of degree less than or equal to $q+2$.*

Now Theorem 1 follows by induction: Let $A^0(f) = T^{[-1,1]}(f)$. Obviously this rule satisfies Assumption 1 with $q = 0$. Assume that the rule $A^m(f)$ satisfies

Assumption 1 with $q = 2m$. Define the rule $A^{m+1}(f) = \widetilde{A^m}(f)$ using (4) with $q = 2m$. By Proposition 2, $A^{m+1}(f)$ satisfies Assumption 1 with $q = 2m + 2$.

By Proposition 1, the rule $A^m(f)$ is actually exact for all polynomials of degree less than or equal to $2m + 1$. Finally note that for $N = 2^m n$ we have $T_{N,m}(f) = (A^m)_n^{[a,b]}(f)$ where $(A^m)_n^{[a,b]}(f)$ denotes the composite rule on $[a, b]$ with n subintervals which is based on the rule A^m. Therefore Theorem 2 implies (1).

Note Theorem 1 remains true if we replace the trapezoid rule by any other symmetric rule.

Remark. Romberg integration on triangles can be treated in a similar way: Here the basic rule T uses the function values at the three vertices of the triangle, this rule is exact for polynomials of total degree one or less. For a rule A on a triangle we define the composite rule A_N by dividing the triangle in N^2 congruent smaller triangles and applying the basic rule A on each subtriangle. Assume that the rule A is exact for all polynomials of total degree q or less with q even. Let E and E_2 be the integration errors of A and A_2. If f_{q+1} and f_{q+2} are monomials of total degree $q + 1$ and $q + 2$, respectively, then we obtain

$$E_2(f_{q+1}) = 2^{-(q+2)}E(f_{q+1}), \qquad E_2(f_{q+2}) = 2^{-(q+2)}E(f_{q+2}). \tag{5}$$

Hence the rule $\tilde{A}$ defined by (4) will be exact for polynomials of total degree $q + 2$ or less. To prove (5), consider the triangle with vertices $(0, 0)$, $(1, 0)$ and $(0, 1)$. Then proceed analogously as in (3) and note that one of the four subtriangles is rotated by 180 degrees. Therefore one of the four terms arising from $E_2(f_{q+1})$ has the opposite sign. For $E_2(f_{q+2})$ expand the arising terms in monomials of degree $q + 2$, $q + 1$, and lower order terms. Then the terms of order $q + 1$ will cancel each other since the central subtriangle is rotated by 180 degrees. As the rule $A^0 = T$ is exact for polynomials of degree zero, induction shows that the rule A^m is exact for polynomials of total degree $2m$ or less. Hence the Romberg extrapolations $T_{N,m}$ converge with order $O(N^{-(2m+1)})$. This is one order lower than in the one-dimensional case, and this result cannot be improved. But no symmetry of the underlying rule T is required for this argument, so T can be *any* quadrature rule which is exact for the function 1.

REFERENCES

1. J. N. Lyness, Quadrature over a simplex: Part 2. A representation for the error functional, *SIAM J. Numer. Anal.*, 5 (1978) 870–887.
2. J. Stoer and R. Bulirsch, *Introduction to Numerical Analysis*, Springer-Verlag, New York, 1992.

Department of Mathematics
University of Maryland
College Park, MD 20742
tvp@math.umd.edu

An Elementary Proof that the Borromean Rings Are Non-Splittable

Ollie Nanyes

Linström and Zetterström [1] gave a proof that the Borromean rings (figure 1) could not consist of true circles. In this note, we give an elementary proof (sans algebraic topology) that the Borromean rings are "linked" though no two components are. The tool that we use is the colorability *mod n* of a knot or link diagram. This tool has been presented in honors undergraduate seminars. I have included a discussion of colorability *mod n* though the technique is well known. For example, see Kauffman, Chapter VI [2].

1. DEFINITIONS. A *knot* will be defined as a smooth (or polyhedral) simple closed curve in 3-space R^3. A *link* is defined as a collection of disjoint smooth (or polyhedral) simple closed curves in R^3. Two knots or links K_1 and K_2 are said to be *equivalent* if there is an orientation preserving homeomorphism h: $R^3 \to R^3$ such that $h(K_1) = K_2$. A link L is said to be *splittable* if there exists a smooth (or polyhedral) 3-ball B, an ordering of the components of the link $K_1, K_2, \dots, K_m$ and an integer $0 < k < m$ such that $K_j \subset B$ for $j \leq k$ and $K_i \subset S^3 - B$ for $i > k$. A *diagram* for a knot or link K is an image of a regular projection (all self-intersections are non-tangential (transverse) and are double points) of K onto a plane with crossing information at each double point (p. 215, reference 2). Note that FIGURES 1 and 4 are examples of diagrams. Two knot or link diagrams D_1 and D_2 are said to be *equivalent* if D_1 can be obtained from D_2 by:

1) Deformations of the plane which do not alter the crossing information at each double point and

2) The three Reidemeister moves and their inverses. See FIGURE 2 for an illustration of these.

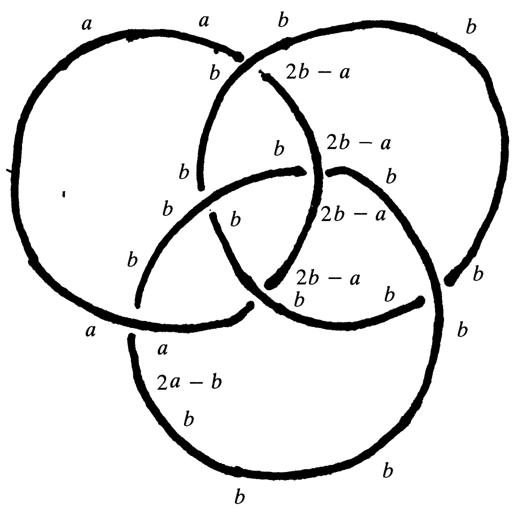


Figure 1

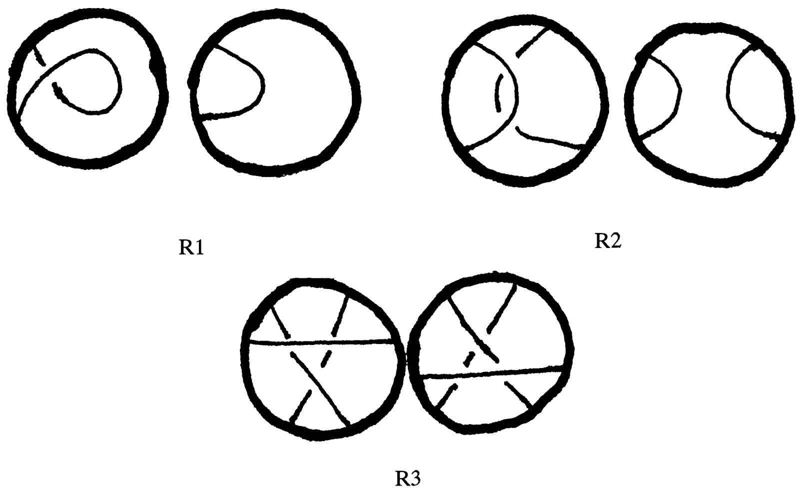


Figure 2. The Reidemeister Moves

2. THEOREMS. The following theorem is well known and will not be proved here.

Theorem 1. *Two knots or links are equivalent if and only if they have equivalent diagrams. See section* 1*B of reference* **[4]** *for a proof.*

A knot or a link K is said to be *colorable* mod n (n is assumed to be 3 or greater) if K has a diagram D in which it is possible to assign an integer to each arc of D which does not contain an undercrossing of D such that:

1) at each crossing we have $a + c = 2b \pmod{n}$ where b is the integer assigned to the overcrossing and a and c are the integers assigned to the other two arcs (see FIGURE 3) and

2) at least 2 distinct integers mod n are used in the diagram.

The following theorem is well known:

Theorem 2. *If K_1 is a knot or a link which is colorable* mod n *then every diagram of K_1 is colorable* mod n.

Proof: Exercise. All one has to check is: if a diagram D is colorable mod n and if one applies either a Reidemeister move (or its inverse) to D, the resulting diagram remains colorable mod n. □

It follows from Theorem 1 and Theorem 2 that if K_1 is a knot or a link which is colorable mod n and K_2 is equivalent to K_1, then K_2 is colorable mod n.

Corollary 3. *There exists a knot which is not equivalent to the unknot.*

Proof: Note that the trefoil knot (see FIGURE 4) is colorable mod 3 whereas the unknot is not. □

We now come to the main result of this note:

Theorem 5. *If a link L is splittable then L is colorable* mod 3.

Proof: If L is splittable with a splitting ball B, then there exists a diagram for L in which the images of $L \cap B$ are separated from the images of $L \cap (S^3 - B)$ by a circle C. Give the components of the diagram of $L \cap B$ the monochrome coloring by assigning the integer 0 to each strand. Similarly, assign the strands of the diagram of $L \cap (S^3 - B)$ the integer 1. $\square$

It is an exercise to see that the standard diagram of the Borromean rings is not colorable mod n for any $n > 1$. The integer labeling of the diagram depicted in FIGURE 1 illustrates this: one has no choice but to set $a = b$. Thus we have an elementary proof that the Borromean rings link is unsplittable and thus the rings cannot be pulled apart.

Remark. If a knot or link K is colorable mod n, then one can obtain a homomorphism from $\pi_1(R^3 - K)$ onto the dihedral group D_n where $D_n = \{s, t | s^2 = 1 = t^n, sts = t^{n-1}\}$. This homomorphism is determined by the particular choice of coloring. See Kaufman [2] or Fox [5].

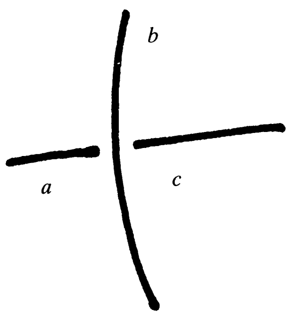


Figure 3

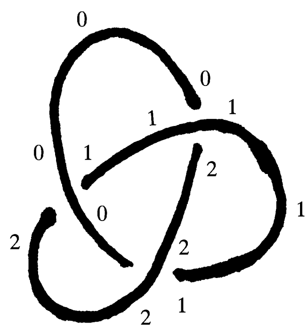


Figure 4

REFERENCES

1. B. Linström and H. Zetterström, Borromean circles are impossible, *American Math. Monthly*, 4(98) (1991) 340–341.
2. L. Kauffman, *Knots and Physics*, World Scientific, New Jersey, 1991.
3. M. A. Armstrong, *Basic Topology*, Springer-Verlag, New York, 1983.
4. H. Zieschang and G. Burde, *Knots*, de Gruyter, New York, 1985.
5. R. H. Fox, A Quick Trip Through Knot Theory, *Topology of Manifolds*, Prentice-Hall 1962.

Department of Mathematics
Bradley University
Peoria, IL 61625
onanyes@bradley.bradley.edu

Letter to the Editor:

Recently Grosof and Taiani [**1**] gave an algebraic proof that if $Q(X) = \prod_1^n (X - r_i)$ with the r_i distinct, then $\Sigma P(r_i)/Q'(r_i) = 0$ for $\deg(P) \leq n - 2$. I should like to add that this result has a home in algebraic number theory, as part of the computation of the "different". The usual proof there [2, p. 135; 3, p.56; 4, p.144] is yet another ingenious algebraic argument. First, standard methods yield the partial fraction decomposition

$$1/Q(X) = \Sigma Q'(r_i)^{-1}/(X - r_i).$$

The right-hand side, as a formal power series in X^{-1}, is

$$\begin{aligned} &X^{-1}\Sigma Q'(r_i)^{-1}/(1 - r_i X^{-1}) \\ &= \Sigma [Q'(r_i)^{-1} r_i^k](X^{-1})^{k+1}. \end{aligned}$$

But the left-hand side is

$$\begin{aligned} &(X^n + a_1 X^{n-1} + \ldots)^{-1} \\ &= X^{-n}(1 + a_1 X^{-1} + \ldots)^{-1} \\ &= X^{-n} - a_1 X^{-(n+1)} + \ldots \end{aligned}$$

Comparing terms, we recover the fact that $\Sigma r_i^k/Q'(r_i) = 0$ for $k \leq n - 2$; we also see that the sum is equal to 1 when $k = n - 1$.

References

1. M. S. Grosof and G. Taiani, Vandermonde strikes again. Amer. Math. Monthly 100 (1993), 575–7.
2. E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen. Leipzig, 1923; reprint Chelsea, New York, 1970.
3. J. P. Serre, Local Fields. Springer-Verlag, New York, 1979. Translation of Corps Locaux, Hermann, Paris, 1962.
4. A. Weil, Basic Number Theory. Springer-Verlag, New York, 1967.

William C. Waterhouse
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802

UNSOLVED PROBLEMS

Edited by: **Richard Guy and Richard Nowakowski**

In this department the MONTHLY presents easily stated unsolved problems dealing with notions ordinarily encountered in undergraduate mathematics. Each problem should be accompanied by relevant references (if any are known to the author) and by a brief description of known partial or related results. Typescripts should be sent to Richard Guy, Department of Mathematics & Statistics, The University of Calgary, Alberta, Canada T2N 1N4.

Open Problems in Pattern Avoidance

James Currie

INTRODUCTION. What makes a mathematical area interesting? The area should contain a range of open problems: some very concrete and approachable, others "bigger". These days it might help for the area to tie in with chaos and fractals. Finally, it couldn't hurt for someone to offer cash for solutions to problems in the area.

A word w over an alphabet Σ is **nonrepetitive** (or squarefree) if no two adjacent blocks in w are identical. For example, the word $v = abcacb$ is nonrepetitive. On the other hand, the word $u = abcbcd$ is repetitive, since bc occurs next to itself in u. Early in this century the Norwegian number theorist Axel Thue showed that arbitrarily long nonrepetitive words can be formed using only three letters [**25**]. Since an infinite tree with finite branching must contain an infinite path, one can also find "infinite words" on three letters which are non-repetitive. We refer to these "infinite words" as **ω-words**.

Thue's result has been rediscovered and republished a dozen times or more. One reason for this sequence of rediscoveries is that nonrepetitive sequences have been used to construct counterexamples in many areas of mathematics: ergodic theory, formal language theory, universal algebra and group theory, for example [**16**, **12**, **6**, **22**].

WORDS AVOIDING PATTERNS. A **word** is a finite sequence of elements of some finite set Σ. We call the set Σ an **alphabet**, the elements of Σ **letters**. The set of all words over Σ is written Σ^*. We take a naive view of words as strings of symbols; thus the concatenation of two words w and v, written wv, is simply the string consisting of the letters of w followed by the letters of v. The **empty word**, with no letters, is denoted by ε.

Let S and T be alphabets. A **substitution** h: $S^* \to T^*$ is a function generated by its values on S. That is, suppose $w \in S^*$, $w = w_1 w_2 \dots w_n$ with $w_i \in S$, $i =$

$1, \ldots, n$. Then $h(w) = h(w_1)h(w_2) \ldots h(w_n)$. We do not allow $h(w_i) = \varepsilon$ for any i. As an example, we could give a substitution h: $\{1, 2, 3\}^* \to \{1, 2, 3\}^*$ by $h(1) = 123$, $h(2) = 13$, $h(3) = 2$. In this case, $h(123) = h(1)h(2)h(3) = 123132$.

A nonrepetitive word over Σ is said to **avoid** xx; it cannot be written $ah(xx)b$ where $a, b \in \Sigma^*$ and h: $\{x\}^* \to \Sigma^*$ is a substitution. Thue also showed that arbitrarily long **cubefree** words on two letters exist [**25**]. Such words avoid xxx in the sense that they cannot be written $ah(xxx)b$. The infinite cubefree word discovered by Thue is referred to as the Morse-Thue sequence, and is an important example in *symbolic dynamics* [**16**, **21**]. Symbolic dynamics is a key tool for studying chaos.

Before posing our problems, we need a bit more background. Let w and p be words. We say that w **contains** pattern p if we can write $w = ah(p)b$ for words a and b, and some substitution h. Otherwise, we say that w **avoids** p. Let a pattern p be fixed. Let Σ be an alphabet with k letters. If there are arbitrarily long words over Σ avoiding p, we say that p is **avoidable on** Σ. Clearly, only the number k of letters in Σ is significant here, so we also say that p is **avoidable on** k **letters**.

For example, xx is avoidable on 3 letters. We say that p *is* **unavoidable** if there is no k for which p is avoidable on k letters. For example, xyx is unavoidable. According to a pretty result of Zimin [**26**], a pattern p on n letters is avoidable if and only if Z_n avoids p, where Z_n is the word on $\{1, 2, \ldots, n\}$ defined by $Z_1 = 1$, $Z_n = Z_{n-1}nZ_{n-1}$, $n > 1$. However, no method is known to determine the smallest alphabet on which p is avoidable [**2**, **3**]. In [**2**], a word U_Δ is given which is avoidable on 4 letters, but not on 3. Perhaps all avoidable words are avoidable on 4 letters.

A word w is **strongly nonrepetitive** if no two adjacent blocks in w are permutations of each other. For example, $u = 512341231416$ is *not* strongly nonrepetitive since the adjacent blocks 12341 and 23141 are permutations of each other. Let p be a word over an alphabet Σ, $p = p_1 p_2 \ldots p_n$, $p_i \in \Sigma$, $i = 1, \ldots, n$. Say that a word w **strongly avoids** p if we cannot write $w = a\hat{p}_1\hat{p}_2 \ldots \hat{p}_n b$ where a, b are words, the $\hat{p}_i$ are nonempty words, and $\hat{p}_i$ is a permutation of $\hat{p}_j$ whenever $p_i = p_j$. Thus a word is strongly nonrepetitive if and only if it strongly avoids xx.

It was known for some time that xx is strongly avoidable on 5 letters, but not on 3 letters [**23**]. It has recently been shown that xx is strongly avoidable on 4 letters [**19**]. On the other hand, the smallest alphabet on which xxx can be strongly avoided is the 3 letter alphabet and the smallest alphabet on which $xxxx$ can be strongly avoided is the 2 letter alphabet [**10**].

Let $a = a_1 a_2 a_3 a_4 \ldots$ and $b = b_1 b_2 b_3 b_4 \ldots$ be ω-words over some alphabet Σ, with $a_i, b_i \in \Sigma$. Define the distance between a and b to be $\rho(a, b) = (1/k)$ where $k = \min\{i \in \mathbb{N} | a_i \neq b_i\}$. Thus the longer a and b go on agreeing, the closer together a and b are. Let L be the set of nonrepetitive ω-words over $\Sigma = \{1, 2, 3\}$. With respect to the metric ρ, L has no isolated points; for any nonrepetitive ω-word a over Σ, we can find distinct nonrepetitive ω-words over Σ agreeing with a to as many places as desired [**24**]. It follows that L is a *Cantor set*.

Concrete Problems

1. Is there a pattern w which is avoidable on 5 letters but not on 4 letters? [**2**]
2. Let L be the set of nonrepetitive words over the 3 letter alphabet $\{1, 2, 3\}$. It is known that $c(n)$, the number of words of L of length n, grows exponentially [**4**]. Give an exact enumeration for L. For the solution to this problem I offer US$100.

3. It is known [15] that the set of cubefree ω-words over a 2-letter alphabet is uncountable. Is the set a Cantor set?

"Bigger" Problems

1. Is there an algorithm which decides, given a pattern p and a natural number k, whether p is avoidable on k letters? [3] If so, give such an algorithm. I offer US\$100 for the solution to this problem.
2. Define **strongly avoidable** in the obvious way. Is there an algorithm which decides, given a pattern p, whether p is strongly avoidable? If so, give such an algorithm. Again, US\$100 to the solver of this problem.
3. Is there an algorithm which decides, given a pattern p and a natural number k, whether p is strongly avoidable on k letters? If so, give such an algorithm. I offer US\$100 for the solution to this problem.
4. For US\$100, decide the following conjecture: If pattern p is avoidable on Σ, then the set of ω-words on Σ avoiding p is a Cantor set.
5. For US\$100, decide the following conjecture: If the smallest alphabet on which p is avoidable is $\{1,2,\dots,k\}$, then there exists a natural number m, and substitutions $f: \{1,2,\dots,m\}^* \to \{1,2,\dots,k\}^*$ and $g: \{1,2,\dots,m\}^* \to \{1,2,\dots,m\}^*$ such that $f(g^n(1))$ avoids p for every $n \in \mathbb{N}$.

REFERENCES

1. S. Arshon, Demonstration de l'existence des suites asymetriques infinies, *Mat. Sb.*, (N.S.) (2) 769–779; *Zbl.* 18, 115.
2. Kirby A. Baker, George F. McNulty and Wayne Taylor, Growth problems for avoidable words, *Theoret. Comput. Sci.* 69 (1989), no. 3, 319–345; *MR* 91f:68109.
3. Dwight R. Bean, Andrzej Ehrenfeucht and George McNulty, Avoidable Patterns in Strings of Symbols, *Pacific J. Math.* 85 (1979) 261–294; *MR* 81i:20075.
4. J. Brinkhuis, Non-repetitive sequences on three symbols, *Quart. J. Math. Oxford* Ser. (2) 34 (1983), 145–149; *MR* 84e:05008.
5. T. C. Brown, Is there a sequence on four symbols in which no two adjacent segments are permutations of each other? *Amer. Math. Monthly* 78 (1971), 886–888.
6. Stanley Burris and Evelyn Nelson, Embedding the dual of π_∞ in the lattice of equational classes of semigroups, *Algebra Universalis*, 1 (1971/72), 248–253; *MR* 45 #5257.
7. James D. Currie, Non-repetitive walks in graphs and digraphs, PhD thesis, University of Calgary (1987).
8. James D. Currie, Which graphs allow infinite non-repetitive walks? *Discrete Math.* **87** (1991) 249–260; *MR* 92a:05124.
9. James D. Currie, Subwords of non-repetitive words, *J. Combin. Theory Ser. A.*, to appear.
10. F. M. Dekking, Strongly non-repetitive sequences and progression-free sets, *J. Combin Theory Ser. A*, 27 (1979) 181–185; *MR* 81b:05027.
12. Andrzej Ehrenfeucht ahd Grzegorz Rozenburg, On the separating power of EOL systems, *RAIRO Inform. Théor* 17 (1983) 13–22; *MR* 84g:68059.
13. P. Erdös, Some unsolved problems, *Magyar Tud. Akad. Mat. Kutato. Int. Kozl.* 6 (1961), 221–254.
14. Roger C. Entringer, Douglas E. Jackson and J. A. Schatz, On non-repetitive sequences, *J. Combin. Theory Ser. A* 16 (1974), 159–164; *MR* 48 #10860.
15. Earl D. Fife, Binary sequences which contain no *BBb*, *Trans. Amer. Math. Soc.* 261 (1980), 115–136; *MR* 82a:05034.
16. Andrés del Junco, A transformation with simple spectrum which is not rank one, *Canad. J. Math.* 29 (1977) 655–663; *MR* 57 #6367.
17. Jacques Justin, Characterization of the repetitive commutative semigroups, *J. Algebra* 21 (1972), 87–90; *MR* 46 #277.
18. Juhani Karhumani, On cube-free ω-words generated by binary morphisms. *Discrete Appl. Math.* 5 (1983), 279–297; *MR* 84j:03081.
19. Veikko Keränen, Abelian squares are avoidable on 4 letters, *Automata, Languages and Programming: Lecture notes in Computer Sciences* 623 (1992) Springer-Verlag, 41–52.

20. Filippo Mignosi, Infinite words with linear subword complexity, *Theoret. Comput. Sci.* 65 (1989), 221–242; *MR* 91b:68093.
21. Marston Morse and Gustav A. Hedlund, Symbolic dynamics I, II, *Amer. J. Math.* 60 (1938) 815–866; 62 (1940) 1–42; *MR* 1, 123d.
22. P. S. Novikov and S. I. Adjan, Infinite periodic groups I, II, III, *Izv. Akad. Nauk. SSSR Ser. Mat.* 32 (1968) 212–244; 251–524; 709–731; *MR* 39 #1531a–c.
23. P. A. B. Pleasants, Non-repetitive sequences, *Proc. Cambridge Philos. Soc.* 68 (1970) 267–274; *MR* 42 #85.
24. Robert O. Shelton and Raj P. Soni, Aperiodic words on three symbols I, II, III, *J. reine angew. Math.* 321; 327; 330 (1981) 195–209; 1–11; 44–52; *MR* 82m:05004a–c.
25. Axel Thue, Über unendliche Zeichenreihen, *Norske Vid. Selsk. Skr. I. Mat. Nat. Kl. Christiana* (1912) 1–67.
26. A. Zimin, Blocking sets of terms, *Mat. Sb.* (*N.S.*) 119 (161) (1982); *Math. USSR Sbornik* 47 (1984) 353–364.

Department of Mathematics
University of Winnipeg
Winnipeg, Manitoba
Canada R3B 2E9
currie@uwpg02.uwinnipeg.ca

Serendipity

After reading the letter to the editor from R. Norwood [The last math journal, Amer. Math. Month., 1993, p. 491–2], I wonder what will happen to those of us who enjoy mathematics, do not have a computer and like to read on public transportation. How will one be able to browse through various items including The American Mathematical Monthly at one's leisure and above all come across the most interesting articles which are always next to those one had planned to read? Will serendipity end?

A. M. Herzberg
Department of Mathematics
and Statistics
Queen's University
Kingston, K7L 3N6
CANADA

PROBLEMS AND SOLUTIONS

Edited by:
Richard T. Bumby, Fred Kochman and Douglas B. West

Proposed problems should be sent to the MONTHLY PROBLEMS address given on the inside front cover. Please include solutions, relevant references, etc. Three copies are requested.

Solutions of published problems should arrive before March 31, 1994 at the MONTHLY PROBLEMS address given on the inside front cover. Solutions should be typed with double spacing, including the problem number and the solver's name and mailing address. Two copies suffice. A self-addressed postcard or label should be included if an acknowledgment is desired.

*An asterisk (*) after the number of a problem, or part of a problem, indicates that no solution is currently available. Partial solutions will be useful in such cases. Otherwise, the published solution is likely to be based on a solution which is complete and correct. Of course, an elegant partial solution or a method leading to a more general result is always useful and welcome. In addition, references to other appearances of MONTHLY problems or to solutions of these problems in the literature are also solicited.*

PROBLEMS

10330. *Proposed by R. Bruce Richter, Carleton University, Ottawa, Ontario, Canada, and Josef Širáň, Technical University of Bratislava, Bratislava, Slovakia.*

Let n and k be given positive integers. Define q, r, s, t to be the unique integers such that $n = qk + r = s(k+1) + t$, with $0 \le r < k$ and $0 \le t \le k$. Show that

$$\binom{q}{2}k + rq \ge \binom{s}{2}(k+1) + ts.$$

10331. *Proposed by Carl Pomerance, University of Georgia, Athens, GA.*

Find all positive integers n such that $n!$ is multiply perfect; i.e., a divisor of the sum of its positive divisors.

10332. *Proposed by Kiran S. Kedlaya, student, Harvard University, Cambridge, MA.*

If n and k are integers with $0 \le k \le n$, prove that

$$\binom{2n}{n+k} = \sum_j 2^{n-k-2j}\binom{n}{j}\binom{n-j}{j+k}.$$

10333. *Proposed by Michael Golomb, Purdue University, West Lafayette, IN.*

For a positive integer n with $2^k \le n < 2^{k+1}$, let $L(n) = 2^k$ $(k = 0, 1, 2, \dots)$. Let $S(n)$ be the sum of the binary digits of n.

(a) Evaluate $\displaystyle\sum_{n \ge 1} \frac{1}{L^2(n) S(n)}$.

(b) Show that $\displaystyle\sum_{n \ge 1} \frac{1}{L(n) S(n)}$ diverges.

(c) Show that $\displaystyle\sum_{n \ge 1} \frac{1}{L(n) S^{1+\delta}(n)}$ converges for every $\delta > 0$.

10334. *Proposed by John Sarli, California State University, San Bernardino, CA.*

Let M be a fixed n by n matrix with complex entries which is *not* nilpotent. For $a, b \in \mathbb{C}$, define the linear operator $M_{a,b}$ on the space of n by n complex matrices by $M_{a,b}(N) = aMN + bNM$. If the operators $M_{a,b}$ and $M_{c,d}$ have the same characteristic polynomial, show that $a^k + b^k = c^k + d^k$ for some k, $1 \le k \le n$.

10335. *Proposed by David Borwein, University of Western Ontario, London, Ontario, Canada, and Jonathan Borwein, Simon Fraser University, Burnaby, British Columbia, Canada.*

Let r be a positive constant and $c_0 \ge 0$. Consider the iteration

$$c_{n+1} = c_n + r - \frac{c_n}{\sqrt{1 + c_n^2}}.$$

(a) For which values of r does the sequence $\langle c_n \rangle$ converge?

(b) In case of convergence to c with $c \ne c_0$, prove that $\lim(c_{n+1} - c)/(c_n - c)$ exists and determine its value.

(c) In case of divergence, find an asymptotic expression for c_n.

10336. *Proposed by Ignacy I. Kotlarski, Oklahoma State University, Stillwater, OK.*

Let $X_1, X_2, \dots$ be a sequence of independent identically distributed random variables, each exponentially distributed with parameter a, $a > 0$, i.e., for $k = 1, 2, \dots,$

$$\mathbf{P}(X_k \le x) = \begin{cases} 0 & \text{if } x \le 0, \\ 1 - e^{-ax} & \text{if } x > 0. \end{cases}$$

Let B be a fixed Borel set in $[0, \infty)$ such that its Lebesgue measure $\mu_L(B)$ is finite and positive. Let

$$Y_k = X_1 + \cdots + X_k$$

for $k = 1, 2, \ldots,$ and

$$\theta = \sum_{k=1}^{\infty} \mathbf{P}(Y_k \in B).$$

(a) Find θ as a function of a.

(b) Find a uniform minimum variance unbiased estimator of θ from a sample from the above exponential distribution of a fixed size n.

10337. *Proposed by Horst Alzer, Waldbröl, Germany.*

Let $n \geq 1$ be an integer. Let $x_1, \ldots, x_n$ be real numbers with $x_i \in (0, 1/2]$. Consider the statement

$$\prod_{i=1}^{n} \frac{x_i}{1 - x_i} \leq \frac{\sum_{i=1}^{n} x_i^n}{\sum_{i=1}^{n} (1 - x_i)^n}. \qquad (\mathbf{F}_n)$$

(a) Prove $\mathbf{F}_n$ for $n \leq 3$.

(b) Show that $\mathbf{F}_n$ is false for $n \geq 6$.

(c) *What about $\mathbf{F}_4$ and $\mathbf{F}_5$?

NOTES

Notes: (10332) The sum may be considered as a sum over all integers j by using the convention that a binomial coefficient $\binom{a}{b}$ is zero unless $0 \leq b \leq a$. **(10337)** The inequality $\mathbf{F}_n$ was suggested by the related statement

$$\prod (x_i/(1 - x_i))^{1/n} \leq \sum x_i \Big/ \sum (1 - x_i),$$

with $i = 1 \ldots n$ in all sums and products. This statement is true for all $n \geq 1$ under the conditions given in the statement of the problem. More information on this inequality, due to Ky Fan, can be found in E. F. Beckenbach and R. Bellman, *Inequalities*.

SOLUTIONS

Alternating Parity in Chebyshev Systems

E 3456 [1991, 646]. *Proposed by A. S. Cavaretta, Kent State University, Kent, OH.*

Suppose $0 = m_0 < m_1 < \cdots < m_n$ are integers such that $m_i \equiv i \pmod 2$.

(i) Prove that a real polynomial

$$c_0 + c_1 x^{m_1} + \cdots + c_n x^{m_n}, \quad \text{with } c_0 c_n \neq 0$$

has at most n real zeros, each zero being counted according to its multiplicity.

(ii) Prove that the generalized Vandermonde determinant

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0^{m_1} & x_1^{m_1} & \cdots & x_n^{m_1} \\ \vdots & \vdots & \cdots & \vdots \\ x_0^{m_n} & x_1^{m_n} & \cdots & x_n^{m_n} \end{vmatrix}$$

is non-zero if $x_0, x_1, \dots, x_n$ are any $n + 1$ distinct real numbers.

Solution by Thomas Kunkle, College of Charleston, Charleston, SC. Part (i): Let $p(x)$ be the polynomial in question. We say that the sequence

$$c_0, c_1, c_2, \dots, c_n \tag{1}$$

has a *sign change* at i ($0 \le i < n$), if, for some $k \ge 1$, $c_i c_{i+k} < 0$, and if, for every j strictly between i and $i + k$, $c_j = 0$. By Descartes's Rule of Signs, the number of positive zeros of $p(x)$ (counted according to multiplicity) is at most the number of sign changes of (1), and the number of negative zeros is at most the number of sign changes of

$$c_0, -c_1, c_2, \dots, (-1)^n c_n. \tag{2}$$

Since $p(0) \neq 0$, to prove (i), we need only show that the number of sign changes of (1) and that of (2) sum to at most n.

By i we will always mean a nonnegative integer, strictly less than n, for which $c_i \neq 0$. By definition, a sign change can occur only at such i. Because $c_0 c_n \neq 0$, for every i there exists a $k = k(i)$ such that $c_i c_{i+k} \neq 0$, and, for all j strictly between i and $i + k$, $c_j = 0$. If $k = 1$, then exactly one of (1) and (2) will have a sign change at i, and if, instead, $k > 1$, then both (1) and (2) might have a sign change at i. Thus the total number of sign changes is less or equal to the number of i for which $k(i) = 1$ plus twice the number of i for which $k(i) \ge 2$. This is less or equal to $\Sigma_i k(i) = n$. This completes the proof of (i).

Part (ii): Suppose that the determinant is zero, or, equivalently, that there exists a nontrivial polynomial

$$p(x) = c_0 + c_1 x^{m_1} + \cdots + c_n x^{m_n}$$

vanishing at the points $x_0, \dots, x_n$. If c_0 is not zero, then, by part (i) of this problem, the number of real zeros of $p(x)$ cannot exceed $\max\{k\colon c_k \neq 0\} \le n$, a contradiction. If, instead, c_0 is zero, we set $l := \min\{k\colon c_k \neq 0\}$, and rewrite $p(x)$ as x^{m_l} times

$$q(x) := c_l + c_{l+1} x^{m_{l+1} - m_l} + \cdots + c_n x^{m_n - m_l}.$$

Since at least n of the points $x_0, \dots x_n$ are nonzero, $q(x)$ has n real zeros. This also contradicts part (i), according to which $q(x)$ has at most $\max\{k - l\colon c_k \neq 0\} \le n - 1$ real zeros. Thus the determinant cannot be zero.

Editorial comment. After the problem appeared, the proposer learned from E. Passow that part (i) had already appeared, with various generalizations, in E. Passow, "Alternating parity of Tchebycheff systems," *J. Approx. Theory* 9 (1973), 295–298. Related results are contained in E. Passow, "Extended Chebycheff systems on $(-\infty, \infty)$," *SIAM J. Math. Anal.* 5 (1974), 762–763. The solver suggested G. Pólya and G. Szegö, *Problems and Theorems in Analysis*, Vol. II, Springer-Verlag, 1972–76 for information on Descartes's Rule of Signs.

Solved also by D. W. Bailey, S.-J. Bang (Korea), D. Callan, R. J. Chapman (U.K.), P. Čižek (student, Czech Republic), T. C. Craven, M. Dindos (Slovakia), J. Duemmel, N. J. Fine, F. Flanigan, L. L. Gardner, H. W. Guggenheimer, Y. Ikeda, A. A. Jagers (The Netherlands), X. F. Jiang (China), I. Kastanas, K. S. Kedlaya (student), D. W. Koster, O. P. Lossers (The Netherlands), R. Martin (student), J. S. Muldowney (Canada), R. J. Neuhaus, J. H. Nieto (Venezuela), A. Nijenhuis, A. Pechtl (Germany), A. Pedersen (Denmark), F. C. Rembis, J. Rickert, M. Roth & O. Šuch (Canada), E. T. Wong, and the proposer.

Restricted Block-Walking

E 3465 [1991, 852]. *Proposed by Dragomir Ž. Đoković, University of Waterloo, Waterloo, Ontario, Canada.*

Let p, q, m, and n be given non-negative integers. Compute the number of sequences of $m + n + 1$ integers $k_{-m}, k_{-m+1}, \ldots, k_{-1}, k_0, k_1, \ldots, k_{n-1}, k_n$ satisfying

(i) $-p \le k_{-m} \le k_{-m+1} \le \cdots \le k_n \le q$.
(ii) $k_{-1} \le 0 \le k_1$.

Solution by William Y. C. Chen, Los Alamos National Laboratory, Los Alamos, NM. The answer is

$$\binom{m+p}{m}\binom{n+q+1}{n+1} + \binom{m+p}{m+1}\binom{n+q}{n}.$$

Recall that the number of nondecreasing sequences of r integers confined to an interval of s integers is $\binom{s+r-1}{r}$ (selections of r integers from s types with repetitions allowed). Now consider two cases: (1) $k_0 \ge 0$, or (2) $k_0 \le -1$. In each case, the desired sequences are built by solving two selection problems. In Case (1), we have

$$-p \le k_{-m} \le \cdots \le k_{-1} \le 0 \quad \text{and} \quad 0 \le k_0 \le k_1 \le \cdots \le k_n \le q.$$

In Case (2), we have

$$-p \le k_{-m} \le \cdots \le k_{-1} \le k_0 \le -1 \quad \text{and} \quad 0 \le k_1 \le \cdots \le k_n \le q.$$

In Case (1), we take m elements from $p + 1$ and $n + 1$ from $q + 1$; in Case (2), we take $m + 1$ elements from $p + 1$ and n from $q + 1$. Together, we have the formula claimed.

Solved also by S.-J. Bang (Korea), J. C. Binz (Switzerland), D. Callan, R. J. Chapman (U.K.), M. Dindos (Slovakia), J. Fukuta (Japan), K. S. Kedlaya (student), E. F. Knapp, A. Nijenhuis, R. B. Richter (Canada), A. Tissier (France), M. Vowe (Switzerland), Anchorage Math Solutions Group, National Security Agency Problems Group, and the proposer. Two incorrect solutions were received.

Strong Fixed Points of Permutations

E 3467 [1991, 853]. *Proposed by Todd Feil, Denison University, Granville OH, and Gary Kennedy, Oberlin College, Oberlin OH.*

A permutation π on the set $\{1, 2, \ldots, n\}$ is said to have j as a *strong fixed point* if $\pi(k) < j$ for $k < j$ and $\pi(k) > j$ for $k > j$. Let $h(n)$ be the number of permutations on $\{1, 2, \ldots, n\}$ having at least one strong fixed point. Prove that

$$2(n-1)! - (n-2)! \le h(n) \le 2(n-1)!$$

for $n > 1$.

Solution by David Callan, University of Wisconsin, Whitewater, WI. For the lower bound, note that 1 and n are strong fixed points for $(n-1)!$ permutations, and $(n-2)!$ of these have been counted twice. For $n \le 4$, equality holds, since 1 or n is a strong fixed point whenever 2 or $n-1$ is a strong fixed point. For $n \ge 5$, both inequalities are strict.

The permutations that do not fix 1 or n cannot strongly fix 2 or $n-1$. We bound the contributions for $3 \le j \le n-2$. The permutations that strongly fix j but not 1 or n permute $\{1, \ldots, j-1\}$ without fixing 1 and $\{j+1, \ldots, n\}$ without fixing n; there are $[(j-1)! - (j-2)!][(n-j)! - (n-j-1)!] = (j-2)(j-2)!(n-j-1)(n-j-1)!$ of these. By comparing successive terms, one notes that this is maximized at the extremes. With $(n-4)$ choices for j, the additional contributions are bounded by $(n-4)(n-4)(n-4)! < (n-2)!$, as required.

Editorial comment. B. M. M. de Weger found the asymptotic expansion

$$2(n-1)! - (n-2)! + 2(n-3)! + 4(n-4)! + 22(n-5)!$$
$$+ 125(n-6)! + 834(n-7)! + O((n-8)!)$$

for $h(n)$. Although there is no simple exact formula for $h(n)$, the generating function $\Sigma_{n=0}^{\infty} h(n)x^n = F(x)/(1 + xF(x))$, where $F(x) = \Sigma n!x^n$, appears in R. P. Stanley, *Enumerative Combinatorics*, Vol. I (Wadsworth and Brooks/Cole 1986), Exercise 32b, pages 49 and 61.

Solved also by R. J. Chapman (U.K.), W. Y. C. Chen, P. Čižek (student, France), R. High, N. Komanda, D. W. Koster, O. P. Lossers (The Netherlands), H. M. Marston, I. Praton, R. W. Sheets, A. Tissier (France), R. Tschiersch (Germany), D. B. Tyler, K. Wayland, B. M. M. de Weger (The Netherlands), National Security Agency Problems Group, University of Wyoming Problem Circle, and the proposer. Three incorrect solutions were received.

Primitive Trigonometric Power Sums

E 3468 [1991, 853]. *Proposed by Curtis Cooper, Central Missouri State University, Warrensburg, MO, Robert E. Kennedy, Central Missouri State University, and Stanley Rabinowitz, Westford, MA.*

Suppose m and n are positive integers such that all prime factors of n are larger than m.

(a) Prove that

$$\sum_{k=1}^{n}{}^{*} \sin^{2m}\left(\frac{k\pi}{n}\right) = \frac{\phi(n) - \mu(n)}{4^m}\binom{2m}{m},$$

which * denotes summation over integers relatively prime to n. (Here ϕ and μ denote the arithmetic functions of Euler and Möbius, respectively.)

(b) Find a similar formula for

$$\sum_{k=1}^{n}{}^{*} \cos^{2m}(k\pi/n).$$

Solution by Kevin Ford, student, University of Illinois, Urbana, IL. For part (b) we show that

$$\sum_{k=1}^{n}{}^{*} \cos^{2m}\left(\frac{k\pi}{n}\right) = \frac{\phi(n) - \mu(n)}{4^m}\binom{2m}{m} + \mu(n).$$

For part (a), the standard binomial expansion yields

$$\sum_{k=1}^{n}{}^{*}\sin^{2m}\left(\frac{k\pi}{n}\right) = \sum_{k=1}^{n}{}^{*}\left(\frac{e^{\pi ik/n} - e^{-\pi ik/n}}{2i}\right)^{2m}$$
$$= \frac{(-1)^m}{4^m}\sum_{k=1}^{n}{}^{*}\sum_{j=-m}^{m}(-1)^{m+j}\binom{2m}{m+j}e^{(m+j-(m-j))ik\pi/n}$$
$$= \frac{1}{4^m}\sum_{j=-m}^{m}(-1)^j\binom{2m}{m+j}\sum_{k=1}^{n}{}^{*}e^{2\pi ijk/n}.$$

If $j = 0$, then $\sum_{k=1}^{*n}e^{2\pi ijk/n} = \sum_{k=1}^{*n}1 = \phi(n)$. If $j \neq 0$, the hypotheses of the problem imply that $(j, n) = 1$, hence as k runs through the set of reduced residues modulo n, so does $h = jk$. In this case,

$$\sum_{k=1}^{n}{}^{*}e^{2\pi ijk/n} = \sum_{h=1}^{n}{}^{*}e^{2\pi ih/n} = \sum_{h=1}^{n}e^{2\pi ih/n}\sum_{d|(h,n)}\mu(d)$$
$$= \sum_{d|n}\mu(d)\sum_{l=1}^{n/d}e^{2\pi ild/n}$$
$$= \mu(n)e^{2\pi i} + \sum_{\substack{d|n\\ d>1}}e^{2\pi id/n}\left(\frac{1 - e^{2\pi i}}{1 - e^{2\pi id/n}}\right)$$
$$= \mu(n).$$

Splitting off the term for $j = 0$ first, we see that

$$\sum_{k=1}^{n}{}^{*}\sin^{2m}\left(\frac{k\pi}{n}\right) = \frac{\phi(n)}{4^m}\binom{2m}{m} + \frac{\mu(n)}{4^m}\left((1 + (-1))^{2m} - \binom{2m}{m}\right)$$
$$= \frac{\phi(n) - \mu(n)}{4^m}\binom{2m}{m}.$$

To obtain (b), we proceed as in part (a). This gives

$$\sum_{k=1}^{n}{}^{*}\cos^{2m}\left(\frac{k\pi}{n}\right) = \sum_{k=1}^{n}{}^{*}\left(\frac{e^{\pi ik/n} + e^{-\pi ik/n}}{2}\right)^{2m}$$
$$= 4^{-m}\sum_{j=-m}^{m}\binom{2m}{m+j}\sum_{k=1}^{n}{}^{*}e^{2\pi ijk/n}$$
$$= \frac{\phi(n)}{4^m}\binom{2m}{m} + 4^{-m}\mu(n)\sum_{\substack{j=-m\\ j\neq 0}}^{m}\binom{2m}{m+j}$$
$$= \frac{\phi(n) - \mu(n)}{4^m}\binom{2m}{m} + \mu(n),$$

since

$$\sum_{\substack{j=-m\\ j\neq 0}}^{m}\binom{2m}{m+j} = 2^{2m} - \binom{2m}{m}.$$

Editorial comment. The proposers included a reference to Stanley Rabinowitz, "Problem 1463," *Crux Mathematicorum*, [1989, 207; 1990, 280], which dealt with a similar sum without the restriction to values of k relatively prime to n. In that form, one is essentially identifying the constant term of the Fourier series of $\cos^{2m}(x)$. This could be generalized to a use of the entire Fourier series of this function as a Discrete Fourier transform. Brian Conolly supplied a reference to B. W. Conolly and I. J. Good, "A table of discrete Fourier transform pairs", *SIAM J. Appl. Math.*, 32 (1977), 810–822, which organizes work on this and similar formulas. In this context, the key steps in solving the present problem amount to the calculation of the transform of the characteristic function of a reduced set of residues modulo n.

Solved also by J. C. Binz (Switzerland), D. Callan, R. J. Chapman (U.K.), P. Čižek (student, France), C. Efthimiou, N. J. Fine, K. S. Kedlaya (student), D. W. Koster, L. E. Mattics, A. Pedersen (Denmark), G. Thompson, J. C. Vera Lizcano (Colombia), Anchorage Math Solutions Group, and the proposers.

An Identity Related to the Landen Transform

6672 [1991, 862]. *Proposed by H. B. Kushner, Nathan S. Kline Institute for Psychiatric Research, Orangeburg, NY.*

If a and b are positive real numbers, prove that

$$\int_0^{\pi/2}\{(a\cos^2\phi + b\sin^2\phi)(a\sin^2\phi + b\cos^2\phi)\}^{-1/2}\,d\phi$$
$$= \int_0^{\pi/2}(a^2\cos^2\theta + b^2\sin^2\theta)^{-1/2}\,d\theta$$

and use it to prove that the integral on the right is unchanged if a and b are replaced by $(ab)^{1/2}$ and $(a+b)/2$, respectively.

Solution by B. W. Conolly, Cambridge, U.K. Let $J(a,b)$ and $I(a,b)$ be the integrals on the left and right, respectively. The substitution $\tan\phi = \sqrt{b/a}\,\tan\theta$ shows that $J(a,b) = I(a,b)$. Moreover, the expression under the radical in $J(a,b)$ can be written

$$(a\cos^2\phi + b\sin^2\phi)(a\sin^2\phi + b\cos^2\phi) = a_1^2\cos^2 2\phi + b_1^2\sin^2 2\phi$$

where $a_1 = (ab)^{1/2}$ and $b_1 = (a+b)/2$. Thus

$$I(a,b) = J(a,b) = \int_0^{\pi/2}(a_1^2\cos^2 2\phi + b_1^2\sin^2 2\phi)^{-1/2}\,d\phi$$
$$= \frac{1}{2}\int_0^{\pi}(a_1^2\cos^2\theta_1 + b_1^2\sin^2\theta_1)^{-1/2}\,d\theta_1 \qquad (\theta_1 = 2\phi)$$
$$= \int_0^{\pi/2}(a_1^2\cos^2\theta_1 + b_1^2\sin^2\theta_1)^{-1/2}\,d\theta_1 = I(a_1,b_1).$$

Editorial comment. Many solvers included material on the arithmetic-geometric mean or elliptic integrals in their proofs. To see the connection with elliptic integrals, assume $a < b$ and set $k = a/b$, $k' = \sqrt{1-k^2}$. Then

$$I(a,b) = \int_0^{\pi/2}(a^2\cos^2\theta + b^2\sin^2\theta)^{-1/2}\,d\theta = \frac{1}{b}\int_0^{\pi/2}(1 - k'^2\cos^2\theta)^{-1/2}\,d\theta$$
$$= \frac{1}{b}\int_0^{\pi/2}(1 - k'^2\sin^2\theta)^{-1/2}\,d\theta = \frac{1}{b}K(k'),$$

where $K = K(k)$ and $K' = K(k')$ are the usual complete elliptic integrals of the first kind for the modulus k. The *Landen Transformation* (see [1], [2] or [4]) states that

$$K'\left(\frac{2\sqrt{k}}{1+k}\right) = \frac{1+k}{2}K'(k). \tag{1}$$

With $k = a/b$, one can check that $(2\sqrt{k}/(1+k)) = a_1/b_1$. Many solvers observed that $I(a_1, b_1) = I(a, b)$ follows from the previous two equations.

Historically, elliptic integrals led to elliptic functions, which in turn led to elliptic curves. From the modern point of view, elliptic integrals are periods of an elliptic curve. To see how this works, consider the elliptic curve E defined by $w^2 = (a^2 + t^2)(b^2 + t^2)$. One can construct E by gluing together two copies of $\mathbb{C} \cup \{\infty\}$ which are cut from ia to ib and from $-ia$ to $-ib$. The cuts allow $w(t)$ to be given by a well-defined function on each sheet. A homology basis of E is $\{\gamma_1, \gamma_2\}$, where γ_1 is $\mathbb{R} \cup \{\infty\}$ on one copy of $\mathbb{C} \cup \{\infty\}$, and γ_2 consists of the segments from $-ia$ to ia on both copies of $\mathbb{C} \cup \{\infty\}$. Since

$$\frac{dt}{w} = \frac{dt}{\sqrt{(a^2+t^2)(b^2+t^2)}}$$

is a nonvanishing holomorphic form on E (unique up to a constant factor), the *periods* of E are the integrals

$$\int_{\gamma_1} \frac{dt}{w} = 2\int_0^\infty \frac{dt}{w} \qquad \int_{\gamma_2} \frac{dt}{w} = 4\int_0^{ia} \frac{dt}{w}.$$

The substitution $t = b\tan\theta$ shows that $\int_0^\infty dt/w = I(a, b)$, so that $2I(a, b)$ is a period of the elliptic curve E. In terms of complete elliptic integrals of the first kind, the periods are

$$\int_{\gamma_1} \frac{dt}{w} = \frac{2}{b}K' \qquad \int_{\gamma_2} \frac{dt}{w} = \frac{4i}{b}K.$$

We can also reconstruct E from its periods as follows. The quotient

$$\tau = \frac{\int_{\gamma_2} dt/w}{\int_{\gamma_1} dt/w} = \frac{2iK}{K'} \in \mathfrak{h} = \{x + iy \in \mathbb{C} \colon y > 0\}.$$

is sometimes called the *period* of E, and there is a complex analytic isomorphism $E \simeq \mathbb{C}/[1, \tau]$ which can be given explicitly in terms of the Jacobi elliptic functions sn, cn and dn. It follows that E is uniquely determined by τ modulo the action of $SL(2, \mathbb{Z})$ on $\mathfrak{h}$.

The identity $I(a, b) = I(a_1, b_1)$ relates E to the elliptic curve E_1 defined by the equation $w_1^2 = (a_1^2 + t_1^2)(b_1^2 + t_1^2)$. The substitutions used in the solution of the problem were $\tan\theta = \sqrt{a/b}\,\tan\phi$ and $\theta_1 = 2\phi$. To get to the elliptic curves, we use $t = b\tan\theta$ and $t_1 = b_1\tan\theta_1$. The resulting change of variables is $t_1 = 2a_1b_1t/(a_1^2 - t^2)$, which comes from a map of the underlying elliptic curves since

$$t_1 = \frac{2a_1b_1t}{a_1^2 - t^2} \qquad w_1 = \frac{a_1b_1w(a_1^2 + t^2)}{(a_1^2 - t^2)^2}$$

defines a function $\Phi \colon E \to E_1$. This map preserves the group structure of E and E_1 and is an example of what is called an *isogeny*.

The isogeny Φ is the key to the whole story. Since it has degree two, one period is preserved while the other is doubled. In fact, we have $2\,dt/w = dt_1/w_1$, and since Φ maps a_1 to ∞, and ∞ to 0, we obtain

$$\int_0^\infty \frac{dt}{w} = \int_0^{a_1} \frac{dt}{w} + \int_{a_1}^\infty \frac{dt}{w} = 2\int_0^{a_1} \frac{dt}{w} = \int_0^\infty \frac{dt_1}{w_1}, \tag{2}$$

where one uses $t \mapsto ab/t$ to justify the second equality. This proves $I(a,b) = I(a_1, b_1)$, which in turn implies the Landen Transform (1). Furthermore, Φ takes ia to ia_1, so that

$$2\int_0^{ia} \frac{dt}{w} = \int_0^{ia_1} \frac{dt_1}{w_1}, \tag{3}$$

and thus the other period is doubled as claimed. One can check that this proves the other half of the Landen Transform, namely

$$K\left(\frac{2\sqrt{k}}{1+k}\right) = (1+k)K(k).$$

If we combine (2) and (3), we see that the period of E_1 is

$$\tau_1 = \frac{2\int_0^{ia_1} dt_1/w_1}{4\int_0^\infty dt_1/w_1} = 2\frac{2\int_0^{ia} dt/w}{4\int_0^\infty dt/w} = 2\tau. \tag{4}$$

There is also a connection with the arithmetic-geometric mean of Gauss (see **[1]**, **[2]** or **[3]**). We have $a_1 = \sqrt{ab}$, $b_1 = (a+b)/2$, and if we iterate this construction, we obtain

$$a_{n+1} = \sqrt{a_n b_n} \qquad b_{n+1} = \frac{a_n + b_n}{2} \qquad n = 1, 2, \dots$$

Since a and b are positive, these numbers converge to a common limit which is denoted $\mu = M(a,b)$ (one can also let a and b be arbitrary complex numbers, but convergence is more complicated in this case—see **[3]**). Then the identity $I(a,b) = I(a_1, b_1)$ implies

$$\begin{aligned} I(a,b) &= I(a_1,b_1) = I(a_2,b_2) = \cdots = I(\mu,\mu) \\ &= \int_0^{\pi/2} \frac{d\theta}{\sqrt{\mu^2\cos^2\theta + \mu^2\sin^2\theta}} = \frac{\pi}{2\mu}, \end{aligned} \tag{5}$$

which proves that $I(a,b)M(a,b) = \pi/2$. Since there are other methods for proving this relation between $I(a,b)$ and $M(a,b)$ (see **[2]**), $I(a,b) = I(a_1,b_1)$ becomes a consequence of the obvious identity $M(a,b) = M(a_1,b_1)$. We can also study (5) from the point of view of the underlying elliptic curves. Let E_n be defined by $w^2 = (a_n^2 + t^2)(b_n^2 + t^2)$. Then (4) implies that the period τ_n of E_n is given by $\tau_n = 2^n\tau$, so that $\tau_n \to \infty$. This means that in the moduli space $\mathfrak{h}/SL(2,\mathbb{Z})$, the elliptic curves E_n are "converging" (the technical term is *degenerating*) to a rational curve. Thus the limit integral in (5) is an integral over a rational curve, which is why it is so easy.

The integrals $I(a,b)$ and $J(a,b)$ of this problem have other interpretations as periods. In particular, $I(a,b)$ is a period of a curve (of genus 1) with equations $u^2 = a^2x^2 + b^2y^2$ and $x^2 + y^2 = 1$, while $J(a,b)$ is a period of a curve (of genus 3) with equations $u^2 = (a^2x^2 + b^2y^2)(b^2x^2 + a^2y^2)$ and $x^2 + y^2 = 1$. The changes of variable in the integrals can then be explained in terms of functions between these curves.

REFERENCES

1. G. Almkvist and B. Berndt, "Gauss, Landen, Ramanujan, the arithmetic-geometric mean, ellipses, π, and the *Ladies Diary*," this MONTHLY 95 (1988), 585–608.
2. J. Borwein and P. Borwein, *Pi and the AGM*, John Wiley & Sons, New York, 1987.
3. D. Cox, "The arithmetic-geometric mean of Gauss," *L'Enseign. Math.* 30 (1984), 275–330.
4. E. Whittaker and G. Watson, *A Course of Modern Analysis*, Fourth Edition, Cambridge University Press, Cambridge, 1963.

Solved also by J. Anglesio (France), F. Bachmann (Switzerland), S.-J. Bang (Korea), R. Betts (student), K. V. Bhagwat (India), P. Bracken (Canada), W. A. Businger (Switzerland), R. J. Chapman (U.K.), Y. Diao, M. Dresević & N. Cakić (Yugoslavia), Z. Guan & N. Passell, R. W. Hopper, D. Jespersen, I. Kastanas, P. Landweber, H. Lipman, N. J. Lord (U.K.), O. P. Lossers (The Netherlands), J. Melville (U.K.), G. Miller (student, Canada), A. Pechtl (Germany), C. E. Rieck Jr. & M. Q. Rieck, T. Schira (Germany), D. Trautman, R. L. Young, K. Zacharias (Germany), University of South Alabama Problem Group, and the proposer.

An All-Ones Problem

10197 [1992, 162]. *Proposed by Uri Peled, University of Illinois, Chicago, IL.*

Light bulbs $L_1, L_2, \ldots, L_n$ are controlled by switches $S_1, S_2, \ldots, S_n$. Switch S_i changes the on/off status of light L_i and possibly the status of some other lights. Assume that if S_i changes the status of light L_j, then S_j changes the status of light L_i. Initially all the lights are off. Prove that it is possible to operate the switches in such a way that all the lights are on.

Solution by O. P. Lossers, Eindhoven University of Technology, Eindhoven, The Netherlands. Define the matrix A as

$$A_{ij} = \begin{cases} 1 & \text{if switch } S_i \text{ controls bulb } L_j \\ 0 & \text{otherwise.} \end{cases}$$

Then A is a symmetric (0, 1)-matrix with all-one diagonal, and it should be proved that the all-one vector belongs to the column space of A, when calculated modulo 2.

More generally we shall prove that for a symmetric binary matrix A the diagonal $\underline{d}$ belongs to the column space modulo 2, denoted Im A. In this form the problem occurs as "Problem 798," *Nieuw Archief voor Wiskunde*, (4) 9 (1991), 117–118. We give a different solution

$$\underline{d} \in \operatorname{Im} A \text{ is equivalent to } (\operatorname{Im} A)^{\perp} \subseteq \langle \underline{d} \rangle^{\perp} .$$

So let $\underline{x} \in (\operatorname{Im} A)^{\perp}$, i.e. $\sum_{i=1}^{n} x_i A_{ij} = 0$ for all j.

Hence $\sum_{i=1}^{n} \sum_{j=1}^{n} x_i A_{ij} x_j = 0$, which, by symmetry of A reduces to $\sum_{i=1}^{n} x_i^2 A_{ii} = 0$. So $\sum_{i=1}^{n} x_i d_i = 0$ since $A_{ii} = d_i$ by definition and $x_i^2 = x_i$. Thus $\underline{x} \in \langle \underline{d} \rangle^{\perp}$ as required.

Editorial comment. Most solvers used a matrix interpretation as above, but a few worked directly with a graph with incidence matrix A. The proposer, in consultation with N. Alon and L. Lovász was able to trace this form of the result to an unpublished result of T. Gallai (see L. Lovász, *Combinatorial Problems and Exercises*, North-Holland, 1979, Exercise 5.17). Other readers provided references to K. Sutner, "The σ-game and cellular automata," this MONTHLY, 97 (1990), 24–34; F. Galvin, "Solution to problem 88-8," Mathematical Intelligencer 11

(1989), 31–32; and K. Sutner, "Linear cellular automata and the Garden-of-Eden," Mathematical Intelligencer 11 (1989), 49–53 (especially theorem 3.2).

Solved by 41 readers and the proposer.

Products of Nilpotent Matrices

10200 [1992, 163]. *Proposed by Daniel Goffinet, St. Étienne, France.*

(a) Prove that a (square) matrix over a field F is singular if and only if it is a product of nilpotent matrices.

(b) If $F = \mathbb{C}$, prove that the number of nilpotent factors can be bounded independently of the size of the matrix.

Solution by Richard Stong, University of California, Los Angeles, CA. We will show that for any field F four nilpotent factors suffice. Clearly a product of nilpotent matrices is singular. Hence we need only decompose a singular matrix into nilpotent factors.

Lemma 1. *If A is a square matrix over F, then A is a product of two matrices that can put into Jordan canonical form with eigenvalues in F. If A is singular, we may further assume that the Jordan canonical forms have a final row and a final column of zeroes.*

Proof: Passing to a different basis, we may assume A breaks up into blocks of the form

$$B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -b_0 & -b_1 & -b_2 & \cdots & -b_{r-1} \end{pmatrix},$$

where the characteristic polynomial $p(t) = t^r + b_{r-1}t^{r-1} + \cdots + b_0$ is a power of an irreducible polynomial. If $b_0 \neq 0$ (i.e., $P(t) \neq t^r$), consider the identity

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ c_1 & c_2 & \cdots & c_{r-1} & c_r \end{pmatrix}^{-1}$$

$$\times \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & 1 \\ -c_r b_0 & c_1 - c_r b_1 & \cdots & \cdots & c_{r-1} - c_r b_{r-1} \end{pmatrix}.$$

For any $\{c_i\}$ the first matrix can be put in Jordan canonical form since its characteristic polynomial is $(t-1)^{r-1}(t-c_r)$. The characteristic polynomial of the second factor is $p'(t) = t^r + (c_r b_{r-1} - c_{r-1})t^{r-1} + (c_r b_{r-2} - c_{r-2})t^{r-2} + \cdots + c_r b_0$. By choosing the c_i appropriately we may assume this polynomial is

$(t - 1)^r$, hence splits over F. If A is singular, then we also get some blocks of the form

$$N = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

For these use the identity

$$N = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & -1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ (-1)^r & (-1)^{r-1} & (-1)^{r-2} & \cdots & -1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}$$

$$\times \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Note that both sides have 0 as an eigenvalue of multiplicity one. Hence both of their Jordan canonical forms have a final row and final column of zeroes. This shows that A is the product of two matrices that can be put into Jordan canonical form and if A is singular, then both have a final row and final column of zeroes. (In fact, if the null space of A is r-dimensional, we get the final r rows and final r columns all zero. Another interesting observation is that if F is infinite the proof above can be modified to show that both factors are diagonalizable.) After a change of basis both these factors have the form

$$\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix},$$

where B is $(n - r) \times (n - r)$ upper triangular and 0 denotes a matrix of zeroes, $r \times r$, $(n - r) \times r$, or $r \times (n - r)$, as required. (In fact, B has only nonzero entries on and just above the diagonal.) The following lemma factors these.

Lemma 2. *Let A be an $n \times n$ matrix of the form*

$$\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix},$$

where B is an $(n - r) \times (n - r)$ upper triangular $(r \geq 1)$. Then A is a product of two nilpotent matrices.

Proof:

$$A = \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ I_{n-r} & 0 \end{pmatrix},$$

where I_{n-r} denotes the $(n - r) \times (n - r)$ identity matrix and 0 denotes a matrix

of zeroes, either $r \times r$, $(n - r) \times r$, or $r \times (n - r)$, as required. The first factor is strictly upper triangular the second strictly lower, hence both are nilpotent.

Applying these two lemmas solves the problem.

Editorial comment. Frank Schmidt and Pei Yuan Wu submitted references to Pei Yuan Wu, "Products of nilpotent matrices," *Linear Algebra Appl.* 96 (1987), 227–232. In this article, Wu proves that every singular complex matrix A is a product of two nilpotent matrices, except for the case where A is a 2 by 2 nonzero nilpotent matrix (in which case he shows that such an expression is *never* possible). Wu also provided a reference to T. J. Laffey, "Factorizations of integer matrices as products of idempotents and nilpotents," *Linear Algebra Appl.* 120 (1989), 81–93. In the introduction to this article, Laffey asserts that Wu's result could be extended to arbitrary fields. However, no solution giving a complete argument leading to fewer than four factors over a general field was received.

Solved also by I. Kastanas, J. Sangroniz (Spain), T. Zeanah (part b only), and the proposer.

Answer to Picture Puzzle
(p. 748)

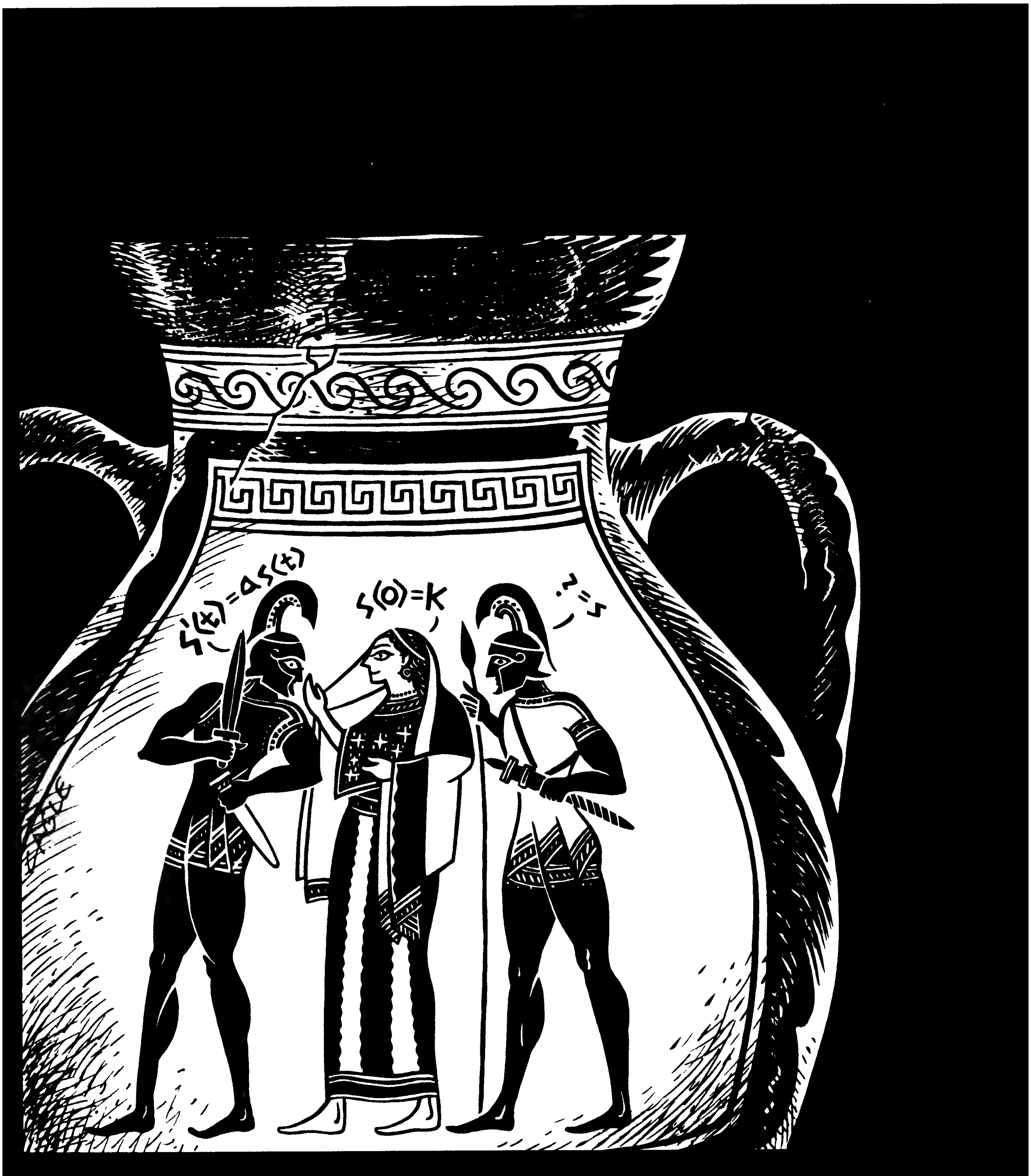
No, they are not: they are Emile Borel and Armand Borel.

Dr. Marston Morse, professor of mathematics at Harvard University, has accepted a call to a professorship of mathematics at the Institute for Advanced Study at Princeton, New Jersey. The staff of the School of Mathematics now consists of the following members: Drs. Albert Einstein, Oswald Veblen, J. W. Alexander, John von Neumann, Herman Weyl and Marston Morse.

42(1935), 124

The American Mathematical Monthly

Volume 100, Number 9 / NOVEMBER 1993



NOTICE TO AUTHORS

The *Monthly* publishes articles, notes, and other features about mathematics and the profession. The readership of the *Monthly* is intended to include everybody who is mathematically inclined, including of course professional mathematicians and students of mathematics at all collegiate levels. While no single article or feature is likely to appeal to everyone, material should interest and be accessible to a large number of readers. This is the most important criterion for acceptance.

Articles may be expositions of old results or presentations of new ones. They may concern all of mathematics or one small area, a broad development or a single application, historical reminiscences or one important event. While some articles may contain the author's new research, the novelty of material and generality of the results is far less important than the clarity of exposition and general interest. Discussing one illuminating case of a well known result is far better than providing all the details of an obscure but new proposition. Articles in the *Monthly* are supposed to inform and to entertain; they are meant to be read rather than archived.

Notes are short and possibly informal articles. A note may concern a clever new proof of an old theorem, a novel way to present tired material, or a lively discussion of a philosophical (but still mathematical) issue. Also, any topic is suitable, so long as it is related to mathematics. Because a note is short, the first few sentences are the most important part: They should explain the purpose and invite the reader in. Photographs or diagrams often will attract the reader's attention.

All articles and notes should be sent to the editor:

JOHN EWING,
Department of Mathematics,
Indiana University,
Bloomington, IN 47405.

Please send 3 copies, typewritten on only one side of the paper. Illustrations should be carefully drawn on separate sheets of paper in black ink; the original should be without lettering and two copies should have appropriate captions and lettering indicated.

Proposed problems or solutions should be sent to:

RICHARD BUMBY,
P.O. Box 10971
New Brunswick, NJ 08906-0971.

Please send 2 copies of all material, typewritten if possible.

Letters to the Editor, both for publication and for private reading, should be sent to the Editor at the address given above. Comments, including criticisms, are welcome, as are all suggestions for making the *Monthly* a lively, entertaining, and informative journal.

Cover:
The title is *ODE on a Grecian Urn*
by John Keats (1795–1821).
Blame and groans should be directed to
Tom Banchoff at Brown University.

Reprint permission:
MARCIA P. SWARD, Executive Director

Advertising Correspondence:
Ms. ELAINE PEDREIRA, Advertising Manager

Subscription correspondence, change of address, and other inquiries:
Membership / Subscriptions Department

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036.

Microfilm Editions: University Microfilms International, Serial Bid coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

The AMERICAN MATHEMATICAL MONTHLY (ISSN 0002-9890) is published monthly except bimonthly June-July and August-September by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, DC 20036 and Montpelier, VT. Second class postage paid at Washington, DC, and additional mailing offices. ***Postmaster***: Send address changes to the American Mathematical Monthly, Membership / Subscription Department, MAA, 1529 Eighteenth Street, N.W., Washington, DC, 20036-1385.

The American
Mathematical Monthly

Volume 100 Number 9 / NOVEMBER 1993
(ISSN 0002-9890)

Contents

ARTICLES

FEATURES

Thomas Archer Hirst—
Mathematician Xtravagant
V. London in the 1860s

J. Helen Gardner and Robin J. Wilson

After leaving the Academy I took my ticket for London by way of Dieppe and Newhaven... The passage was without exception the smoothest I ever made, the Channel was as quiescent as a duck-pond, the day beautiful and sunny... I was right glad to see the white cliffs of my native land and my eyes lingered gladly on the villages with their churches and on the farm-steads about which was an air of solid domestic comfort and prosperity which we look for in vain out of England. In short I felt a quiet pleasure in realising the fact that after long wanderings I was coming home at last and that sources of happiness were in store for me to which I had long been a stranger...

After two years establishing his reputation in Europe, Hirst decided that it was time to return home. On arrival in London, in the summer of 1859, he took up lodgings near John Tyndall.

9th October 1859: ... Indeed my London life commences well. I have John close to me, can run into his rooms half an hour every evening and finish off the day with pleasant useful conversation. Never in my life was I better situated for getting through solid work and having the advantage of the best companionship. I trust the effects of all this will be visible by and bye...

James Joseph Sylvester (1814–1897)

Arthur Cayley (1821–1895)

By now, Tyndall was firmly established in the London scientific scene, and he introduced Hirst into his circle of friends. This enabled Hirst to become acquainted with the major scientific figures of the day. But what might have been merely polite introductions often developed further.

16th October 1859: On Monday having received a letter from [James Joseph] Sylvester I went to see him at the Athenaeum Club. We had an hour's talk in the little waiting room. He talked continuously for that time about his partitions of numbers and strange to say he was less obscure than I expected. He was, moreover, excessively friendly, wished we lived together, asked me to go live with him at Woolwich and so forth. In short he was excentrically affectionate...

Just before Christmas he called on Arthur Cayley, and spent a very interesting hour talking about Cayley's work on curves of the third order and a new method for obtaining the squares of the differences of the roots of a quintic, and his own work on derived curves of double curvature.

23rd December 1859: ... I explained what I was doing in which he expressed some interest. I was a little amused and encouraged too by his asking me for a definition of the rectifying plane. The great geometer had forgotten it for the moment.

What a wonderful head he has, not merely round but spheroidal with the largest diameter parallel to his eyes, or rather to the line joining his ears. He never sits upright on his chair but with his posterior on the very edge he leans one elbow on the seat of the chair and throws the other arm over the back. Yet he is a keen sighted and extraordinary man, gentle I think by nature and at once timid, modest and reticent. Often when he speaks he shuts his eyes and talks as if he were reading from an unseen book, and talks well too so that one has to sharpen one's own wits to follow him.

His reading was wide, ranging from Alfred Tennyson's *Idylls of the King* to George Boole's *Differential Equations*. In the latter he found a passage that seemed to be related to his work.

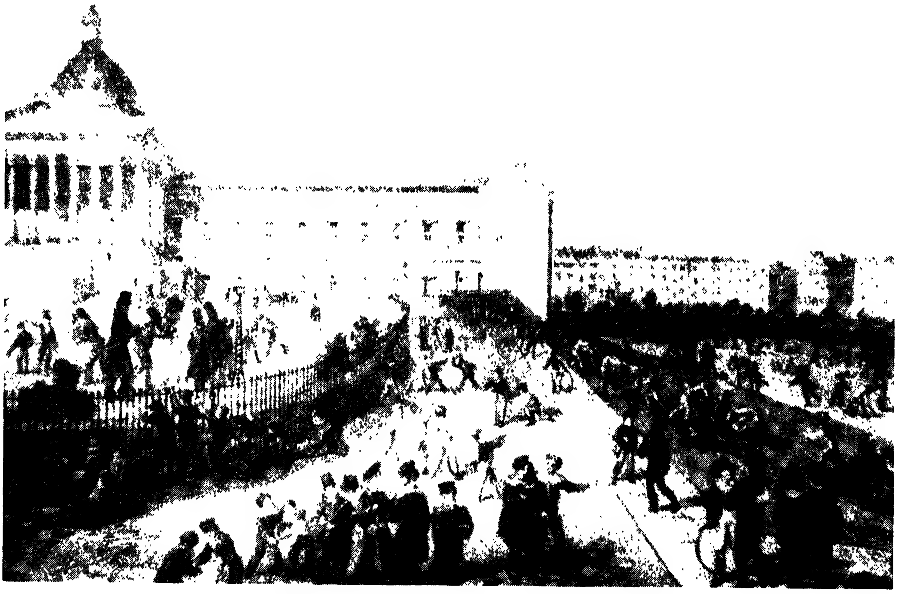
29th January 1860: ... In the chapter on Partial Differential Equations p. 342 occurs this passage "Similar but more interesting applications may be drawn from the problem of the determination of equally attracting surfaces." This shows he has read my Memoir, but my name is not mentioned; yet I think I am the only one who has considered the problem in question.

Hirst also attended lectures of current importance, such as one given by his friend Thomas Huxley on Charles Darwin's recently proposed theory of evolution.

12th February 1860: ... On Friday evening I heard Huxley's lecture on the Origin of Species at the Royal Institution. He gave us a noble peroration which is the part I shall remember longest... Tyndall introduced me to Babbage with whom we walked part of the way home.

Employment for a mathematician was as difficult to obtain as it had been seven years earlier when he returned from Berlin—but again, Hirst fell on his feet, being offered the post of mathematics teacher at the University College School. This was initially a temporary post, which Hirst accepted gladly. The headmaster was the distinguished classical scholar and mathematician Thomas Hewitt Key.

4th March 1860: ... I was introduced by Key to my class on Wednesday morning at 9.15, and have continued to attend ever since. I am occupied there from 9.15 A.M. to 3 P.M. with an interval of an hour and a half at noon. My salary is £1 per day. For a school the instruction is of a superior kind. The highest class is engaged with the 6th book of Euclid, the Binomial Theorem in Algebra, De Moivre's theorem in Trigonometry and the simple machine in mechanics. So far I have succeeded quite well. I have merely been learning their powers.



University College School
Founded in 1833, this school was built on the site of University College, in Gower Street, London, where it remained until moving to its present location in Hampstead in 1907.

...I rise every morning now at 7, breakfast at 7.30, light my pipe at 8 and smoke and attend to other necessary matters connected with health until 8.30, then walk down to Regent Street where I take the Islington omnibus which puts me down at the end of Gower Street within a few minutes walk of the College. At noon I get a chop and glass of sherry where I can and return soon after 3.P.M. by the omnibus pretty well tired. Promising as my position is I should hesitate to accept it as a permanency. The consideration of £1 per day would not induce me to neglect my dear "derived surfaces".

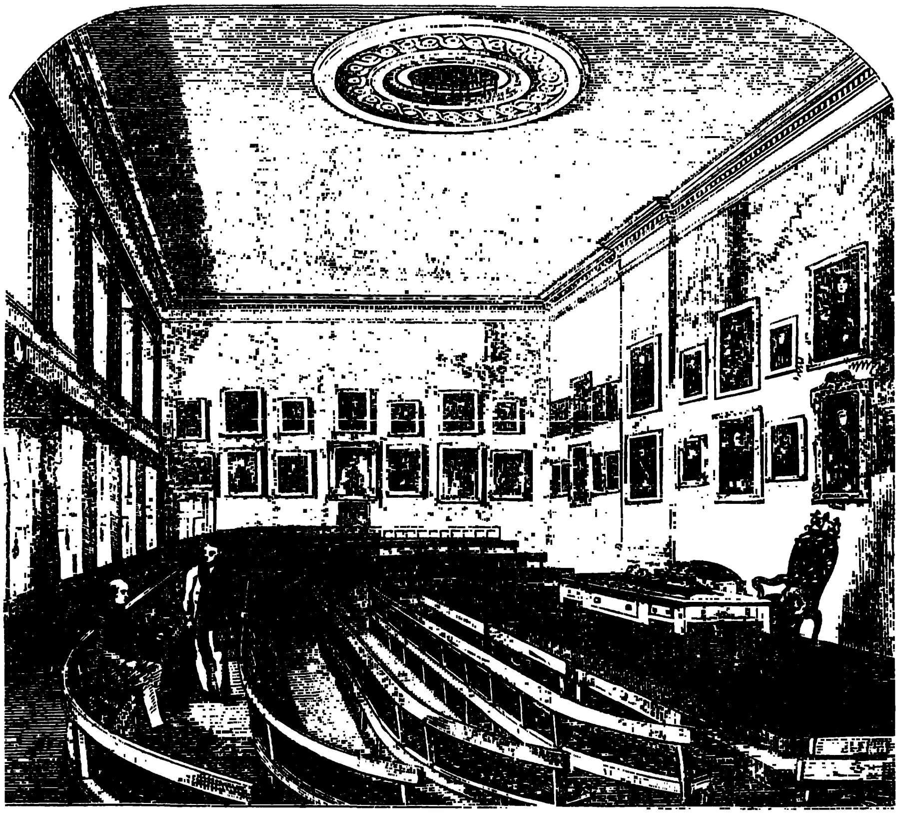
Not long after this, Hirst found himself drawn towards a rather different type of activity.

3rd June 1860: ... a week ago (Friday week) I became enrolled in the Volunteer Guards (6 feet men). I paid one guinea entrance and one guinea subscription in advance. I have been twice to drill once at the house of our Sergeant and Secretary Mr Halse who lives quite near, and once in undress uniform at Hungerford Hall. The uniform is exceedingly conspicuous, a red tunic with black belt and shoulder strap, a black patent-leather helmet (Prussian shape) with black plume and black trousers with red stripe. The undress is a red flannel jacket. I have joined them chiefly for the sake of the drill which I hope will be beneficial but I am also quite prepared to accept all the consequences and in case of need to defend my country with my life. As far as physique is concerned the Guards are a fine body of men about 70 in number, the uniform is expensive and consequently the members are all gentlemen.

In the meantime, Hirst continued, albeit slowly, with his translations and lecturing. His investigations had ground to a standstill, but even so, on March 1861, at the age of only 30, Hirst was nominated for a Fellowship of the Royal Society. His certificate was signed by (among others) Boole and Sylvester. There were many

other candidates, so he was not hopeful.

24th March 1861: ... the Royal Society were discussing my merits. I have two powerful competitors [Henry] Smith of Oxford and [James Clark] Maxwell of King's College; unless all three can be admitted I must expect to be the excluded one... Yesterday I was at an evening party at Dr. Carpenter's and was introduced to Helmholtz and Maxwell with both of whom I had long conversations. The former is a little reserved, the latter talkative with a Scotch brogue, he took great interest in my ripples about which we spoke for some time...



The Royal Society of London
The Royal Society was founded in 1662 by King Charles II. In 1863 it moved into these new rooms in Burlington House, Piccadilly. It is now located in Carlton House Terrace, near St. James's Park.

Figure 3.

Unfortunately, his health was causing him problems. Even after an Easter vacation, he felt exceedingly weak and spiritless. Although he suffered from no particular ailment, he had no energy for either his schoolwork or his researches.

14th April 1861: ... I pay the greatest attention to diet and avoid smoking all day. But instead of being better for such abstinence I feel weaker. I must persevere however for although the two pipes I still allow myself do me good at the time I have a firm belief that for my complaint, indigestion, smoking must be injurious or at least cannot be beneficial. Sooner or later therefore

abstinence must tell upon my health. Who knows how much of my present debility is due to the habit (of 11 or 14 years standing) of smoking five or six times a day. To cut down smoking to two pipes a day has been one of the greatest trials I have gone through, but perseverance diminishes the trial.

A week later, however, he learned from Tyndall that the Council of the Royal Society had placed his name upon the list of candidates to be elected Fellows in June. There were about 45 candidates, only 15 of which were chosen.

21st April 1861: ... Next morning I received the following note from Cayley:
Dear Sir,—I have much pleasure in being able to inform you of your name being on the Council list for the next election of Fellows of the Royal Society.

Believe me yours very sincerely
A. Cayley

... Of course the news was very welcome to me and in reply to Cayley I assured him that the honour would always be enhanced to me by the thought that *his* name was amongst those of the Council who had lent me so generous a support.

In March 1862 he recorded that he had been unable to get through his teaching work at the School. Extreme flatulence had produced giddiness which totally prevented him from standing at the board, and a strange numbness crept over his right arm and leg. It transpired that he had become very ill with dyspepsia, from which he was to suffer for over a month. Happily, he was soon back enjoying the company of his friends.

4th May 1862: ... Yesterday, Saturday, Cayley, Sylvester and Harley dined with me. Tyndall was not present. It was without question to me the most interesting dinner party I ever gave and I believe one of the most successful at least all appeared to enjoy themselves. I contrived to give my three guests opportunities of communicating their latest results. Cayley explained his late controversy with Boole on a question of Probabilities. Sylvester was eloquent on the subject of Reseaux which has now complete possession of him. According to his own confession he is so excited about it that he cannot trust his own critical judgment and has to call Smith of Oxford to his assistance. Harley entered into a few particulars on his Differential Resolvents of Algebraic Equations and I communicated my results on Derived Surfaces which Sylvester pronounced to be at once interesting and 'wonderful'. At 9.30 P.M. we all adjourned (in a cab) to Sabine's Soirée at Burlington House...

He was now making good progress with his investigations. Shortly afterwards, he met Augustus De Morgan and told him of his researches, but received a very cool reception.

15th June 1862: ... He had no better remark to make than 'How did you come across that problem?' There are such an immense variety of similar questions. It was a kind of pooh pooh in fact. I felt angry with myself at having taken him even so much into my confidence. I ought to have *felt* that interest would not be reciprocal. A dry dogmatic pedant I fear is Mr. de Morgan notwithstanding his unquestioned ability...

One of the most important scientific events of 1862 was the meeting of the British Association held at Cambridge, where he made several new acquaintances and presented a short communication on pedal curves which was 'listened to with attention but created no discussion'.

4th October 1862: ... I was much pleased with Boole... Immediately after breakfast I stepped up to him and introduced myself. The same day we sat together at the Hall dinner and had some pleasant chat. Evidently an earnest able and at the same time a genial man.

He was, however, rather less impressed when he subsequently came across the distinguished physicist William Thomson, later Lord Kelvin.

7th June 1863: ... I have attended Thomson's two lectures at the Royal Institution on the Electric Telegraph. More random unsatisfactory lectures I never listened to.

15th June 1863: ... On Tuesday last I was at an "at home" given by Dr. and Mrs. King, the parents of one of my pupils and moreover relations of Prof. W. Thomson of Glasgow. It was the first time I had been introduced to Thomson. I cannot say that we suited one another very well or exchanged many words. He was civil and spoke flatteringly of my papers.

During the late summer, his health began to deteriorate again, making it difficult for him to transfer his thoughts to his researches, and he paid an extended visit to France, Switzerland, Germany, Italy, and Norway. His journal records his sadness at the death of Steiner, as well as meetings with both old and new acquaintances. While in Germany, he attended a gathering of the Naturforschende Gesellschaft, where he met Rudolf Clausius, whose memoirs he had earlier translated.

1st September 1863: ... I seized Clausius and he introduced me to Dedekind, a modest able mathematician Prof. at the Polytechnicum in Braunschweig. After dinner which was enlivened by numerous toasts, Clausius, Dedekind and I took our seats in a vehicle for the Excursion to the Morteratsch Glacier and a very pleasant excursion it was...

The following summer, after completing his year's teaching, he set off on what was becoming an annual visit to the Continent. While in Paris, he dined with Chasles:

16th May 1864: ... The places of honour were given to Tchebichef whose acquaintance I renewed, for years ago I met him at Dirichlet's... On Wednesday Tchebichef called on me and left me some of his papers. He is evidently a good natured man, he has a stuttering way of speaking French and is lame.

... On Friday I took the American Railway to Sevres and sought the Maison Penel where Bertrand is at present residing. He had invited me to dinner... Tchebichef and myself were again the honoured guests on the right and left of Mrs Bertrand, Bertrand himself being opposite. I had much more conversation with Bertrand than I ever had before. I remember I had once a little prejudice against him. His manner I thought a little pretentious and forbidding. I begin to find that this is merely external, the man is kind at heart, extremely clever and full of ésprit...

He particularly enjoyed spending a month in Bologna, where he renewed his acquaintance with Luigi Cremona and attended one of Cremona's lectures.

5th June 1864: ... He had a class of about 12 and lectured on the Theory of the Sun's Dial in connection with his Descriptive Geometry. He is evidently a good lecturer; everything was explained with perfect clearness. One peculiarity of the lecture arrangements was that instead of a black board on the side of the room the top of the table before the professor was of slate and on it he wrote and made figures in chalk. The figures were of course inverted to the audience.

In July 1864, he resigned his post at University College School in order to devote more time to research, and in November, he and Tyndall, along with other close friends, formed themselves into a select scientific club.

6th November 1864: ... On Thursday evening Nov. 3, an event, probably of some importance, occurred at the St George's Hotel, Albemarle Street. A new club was formed of eight members: viz: Tyndall, Hooker, Huxley, Busk, Frankland, Spencer, Lubbock and myself. Besides personal friendship, the bond that united us was devotion to science, pure and free, untrammelled by religious dogmas. Amongst ourselves there is perfect outspokenness, and no doubt opportunities

will arise when concerted action on our part may be of service. The first meeting was very pleasant and "jolly."... There is no knowing into what this club, which counts amongst its members some of the best workers of the day, may grow, and therefore I record its foundation. Huxley in his fun christened it the "Blasto dermic Club" and it may possibly retain the name.

The "jolly" time they had was obviously fruitful, for the X-club, as it became, was to influence the organization and image of English science for the next twenty years. They all acquired nicknames such as the Xcentric Tyndall, the Xalted Huxley and the Xtravagant Hirst.

Three members of the X-club

The Xcentric Tyndall

The Xalted Huxley

The Xtravagant Hirst

In November 1864, Hirst was elected to the Council of the Royal Society for the first time. The very next week saw the first meeting of what was later to become the London Mathematical Society. Hirst became its first Vice-President, and was a member of the Council for almost two decades, becoming its treasurer, and later its President.

13th November 1864: ... On Monday last I attended the first meeting of the Mathematical Society at University College. De Morgan gave an address, which I seconded. I was put upon the Committee. I had at first declined but at De Morgan's request allowed my name to stand.

25th June 1865: ... On Monday I attended the Math. Soc. and proposed Cayley, Sylvester, Spottiswoode and Green as members. Sylvester gave us a capital communication on Newton's rule for the discovery of the imaginary roots of an equation.

On 18th August 1865, he received from the Secretary of University College the news of his appointment as Professor of Mathematical Physics. He had good reason to feel pleased with himself. His appointment to this newly-created chair established him as one of only seven physics professors in the country.

> **28th August 1865:** ... Thus I have reached another step in my career. I have waited long for it and sacrificed much in order to stop in London. I trust I may have health and strength to perform my new duties efficiently.

> **15th October 1865:** On Tuesday morning at 9 my work commenced with a lecture to 25 or 26 students. It passed off well and was listened to with the greatest interest. On Wednesday morning I commenced with my senior class, there were 5 students and a visitor... I have since continued my work every morning and have now altogether about 32 students which represent an income of 162 pounds upon which therefore I shall just be able to live without seeking for extra work.

This point marks the pinnacle of his career. As a Council member of the Royal Society, a member of the X-club, and Vice-President of the London Mathematical Society, he had become a most important member of the Scientific Establishment in London. Regrettably, his fortunes were soon to decline, as we shall see in the final article.

ACKNOWLEDGEMENTS. A typed version of the Thomas Hirst diaries is held at the Royal Institution in London, and quotations from the diaries appear here by courtesy of the Royal Institution. The diaries have been edited by W. H. Brock and R. M. MacLeod, and were published in microfiche by Mansell, London, in 1980.

The Open University
Milton Keynes MK7 6AA
England

Review

Infinitesimal Calculus. By F. S. Carey. (Longmans Mathematical Series.) London, Longmans, 1919. 8 vo. 20 + 352 + 9 pages. Price 14 shillings.

The symbolism referred to for range and sequence is simple and worthy of mention. An open range from a to b is denoted by brackets $[a, b]$, a closed range by parentheses (a, b); and a range open only at one end by the appropriate combination of the bracket and parenthesis symbols; thus a range open at a and closed at b is denoted by $[a, b)$.

—*American Mathematical Monthly* 27, (1920) p. 470–471

From the Post-Markov Theorem Through Decision Problems to Public-Key Cryptography

Iris Lee Anshel and Michael Anshel

Dedicated to the Legacy of Emil Post

1. INTRODUCTION. On November 3–4 1988 a conference to commemorate the life and legacy of Emil Post (1897–1954), in anticipation of his one-hundredth birthday, was held at the City College of New York. Emil Post graduated from the City College in 1917 and received a Ph.D. from Columbia University in 1920. A postdoctoral fellowship at Princeton University was followed by long years of teaching in the public school system. He returned to the City College in 1935 as a member of its Mathematics Department where he resided for the remainder of his academic career. In the process Post was transformed from a brilliant young researcher into a great teacher and visionary intellectual. Four decades after their initial contacts with Post his former students spoke of him with a reverence that is rarely encountered in university life. The scholarly aspects of his commemorative meeting dealt with a wide range of Post's contribution to mathematics, logic and computer science. In this paper we should like to briefly recount his profound influence on the theory of algorithmic decision problems and the connections between this active field of research and current methods in public-key cryptography. We conclude our discussion by posing an historical question concerning the relationship between Post and the cryptologists of his day, the answer to which may shed new light on his legacy in the shadowy world of secret intelligence.

2. STRING REWRITING, THUE SYSTEMS, AND PRESENTATIONS. In this section we briefly review the basic concepts of string rewriting, Thue systems, and presentations. With this language in place we will be in a position to discuss some of the classical decision problems with which Post was concerned.

We begin by motivating this discussion with an historical example, a *Caesar cipher*. Identify the letters of the English alphabet $\{A, B, \dots, Z\}$ with the symbols $\{a_0, a_1, \dots, a_{25}\}$. Consider the set of pairs

$$\{(a_i, a_j) | i - 1 = j \bmod 26\}.$$

These pairs define a method of encrypting plaintext messages: for example 'IBM' $(a_8 a_1 a_{12})$ becomes 'HAL' $(a_7 a_0 a_{11})$ when a_i appearing in the plaintext string is replaced by a_{i-1} to obtain the ciphertext.

The idea behind the above example is to consider an alphabet together with a set of replacement or rewriting rules. With this in mind we begin our formal development. Let A denote a set of symbols (which we shall refer to as an *alphabet*). Consider $FM(A)$ the free monoid based on A. The elements of $FM(A)$ are the finite sequences of symbols or *words* from the alphabet A. Equality in

$FM(A)$ will be denoted by $\rightleftharpoons$; that is given words u and v in $FM(A)$, $u \rightleftharpoons v$ if and only if they denote exactly the same string. Multiplication in $FM(A)$ of the words u, v is simply given by the concatenation uv, and the empty word e serves as the identity in $FM(A)$.

A *rewriting system* RW on A consists of the pair (A, P) where

$$P \subseteq FM(A) \times FM(A).$$

A *derivation* with respect to RW is a finite sequence of words in $FM(A)$,

$$w_1, \ldots, w_n$$

such that either $n = 1$ or for each $i = 1, \ldots, n-1$ there exists

$$x_i, y_i \in FM(A)$$

and

$$(u_i, v_i) \in P$$

such that the equations

$$w_i \rightleftharpoons x_i u_i y_i$$

and

$$w_{i+1} \rightleftharpoons x_i v_i y_i$$

hold. We shall refer to the pair (u_i, v_i) as a *rewriting rule* or *production*, and term w_n *derivable* from w_1.

Returning to the Caesar cipher rewriting system described above, the process of enciphering 'IBM' by 'HAL' is given by the following derivation:

$$a_8 a_1 a_{12}, a_7 a_1 a_{12}, a_7 a_0 a_{12}, a_7 a_0 a_{11}.$$

In his 1947 paper on the algorithmic unsolvability of a problem of Thue, Post introduced a class of combinatorial systems which he called *systems of semi-Thue type* [**21**]. From our perspective these are rewriting systems with finite alphabet and finitely many rewrite rules, together with a specified initial word. The semi-Thue systems serve as a convenient tool to represent the computation of a Turing machine. An exposition of this methodology is given in a now classic text on computability and unsolvability by Martin Davis [**4**], a student of Post and an authority on his life and work.

A *Thue system* T is a rewriting system such that the set P of productions is a symmetric relation on $FM(A)$: if $(u, v) \in P$ then $(v, u) \in P$. The imposition of this symmetry condition insures that the process of deriving (or *rewriting*) the word w_n from w_1 as above is reversible. Fixing our Thue system we now consider the equivalence relation P^* on $FM(A)$ generated by the set of productions P (by definition P^* is the intersection of those equivalence relations on $FM(A)$ which contain P). From the definition of P^*, it follows that two words $FM(A)$ are equivalent provided one is derivable from the other. Moreover P^* is a congruence on $FM(A)$. The semi-group $M(T)$ specified by the Thue system T is thus isomorphic to the factor monoid

$$M(T) \cong FM(A)/P^*.$$

Specifying each production (u, v) and its reverse by the equation $u = v$ we obtain the traditional monoid presentation for $M(T)$,

$$\langle A; u = v((u,v) \in P) \rangle. \tag{2.1}$$

Conversely, it is not difficult to show that given an arbitrary monoid M there exists

some Thue system T such that

$$M \cong M(T).$$

In the case A is finite we say that T and $M(T)$ are *finitely generated*, in the case P is finite we say that T and $M(T)$ are *finitely related*, and the Thue system T and the monoid $M(T)$ are said to be *finitely presented* if they are both finitely generated and finitely related. We will be concerned with finitely presented Thue systems T and we shall denote its associated monoid presentation by

$$\langle a_1, \dots, a_n; u_1 = v_1, \dots, u_k = v_k \rangle. \tag{2.2}$$

A *group alphabet* is an alphabet A partitioned into two disjoint subsets, $A(+)$, the *positive* symbols, $A(-)$, the *inverse* symbols together with an idempotent permutation *inv* of A such that

$$inv \colon A(+) \to A(-).$$

We write $a^{-1} = inv(a)$ for a in A and note $(a^{-1})^{-1} = a$. The notation extends to the words over the group alphabet by taking $e^{-1} = e$, and for $z = b_1 \dots b_t$ setting $z^{-1} = b_t^{-1} \dots b_1^{-1}$ where the b_i are positive or inverse symbols. A word z is said to be freely reduced provided it is not of the form $z = xaa^{-1}y$ or $xa^{-1}ay$ for any a in $A(+)$. A monoid presentation is said to be a *group presentation* provided it is specified by a Thue system over a group alphabet whose rewrite rules satisfy the following conditions:

(i) All rewriting rules of the form $aa^{-1} = e$ and $a^{-1}a = e$ for a in A are contained in the system, and we call these rules *trivial relators*.

(ii) All other rewriting rules or *non-trivial relators* occur in pairs of the form $u = e$, $u^{-1} = e$ where u, u^{-1} are free reduced words.

The collection of all rewriting rules is called the *defining relators*.

In general, the trivial defining relators are suppressed when specifying the group, as are the companions to each non-trivial relator $u = e$. In addition we list only the positive symbols. A finitely presented group G is thus specified and denoted by

$$\langle a_1, \dots, a_n; u_1 = e, \dots, u_k = e \rangle.$$

For an example of a presentation we consider F_n, the free group of rank n, which by definition has no non-trivial relators. We see that F_n is specified by the group presentation

$$\langle a_1, \dots, a_n; \rangle.$$

Every group is a factor group of a free group and may be specified up to isomorphism by a group presentation.

3. ALGORITHMIC DECISION PROBLEMS. By a *decision problem* we mean one whose instances require a yes/no answer. A decision problem is said to have an *algorithmic solution* if it is possible to program a digital computer to correctly supply the yes/no responses. If this is not possible we say that the problem is *algorithmically unsolvable*. If there is such a program and the running time of the program is bounded by a polynomial in the symbolic size of the input then we say the solution is *efficiently constructible*.

The algorithmic concepts referred to above are very natural to our computerized society. This was not the case in 1936 when Post [**19**] as well as Turing [**24**] both formulated a basis for these concepts by specifying idealized computing machines. In Turing's exposition a *universal* computer capable of executing any

algorithm is constructed. The *halting (or stopping) problem* for this machine is then shown to be algorithmically unsolvable. Post **[21]** clarified the construction of Turing's machine and applied his methods in order to resolve a problem of Thue **[23]** which we will discuss in §4.

Perhaps the most widely discussed decision problem of the twentieth century is Hilbert's Tenth Problem. This problem asks for an algorithmic solution for determining whether or not an integral polynomial equation has integer solutions. Post believed that Hilbert's Tenth Problem was algorithmically unsolvable **[20]**. The force of this belief was conveyed to Martin Davis who, along with Hilary Putnam and Julia Robinson, provided the basis for Yuri Matiyasevich's proof of its algorithmic unsolvability **[14]**. Martin Davis was cited by Marvin Minsky at his address to the City College conference as directing his (Minsky's) attention to Post's problem of *tag*. Minsky went on to show that this problem was algorithmically unsolvable **[17]**. Researchers such as Davis and Minsky have enabled Post's ideas to be transferred and transformed by succeeding generations. This process has made possible the enormous advances in *computer science* that have allowed it to emerge as an academic discipline.

4. THE POST-MARKOV THEOREM AND SUBSEQUENT DEVELOPMENTS. We now restrict our attention to finitely presented monoids and groups. In the following discussion, we fix a presentation for the monoid or group in question. The *word problem* for a finitely presented monoid (resp. group) is to decide for arbitrary words, w, z in the alphabet (resp. group alphabet) whether or not the words are congruent via the associated Thue system (resp. group presentation).

Thue's word problem for finitely presented monoids appears in a 1914 paper of A. Thue **[23]** while the word problem for groups is formulated in the course of a topological investigation in 1911 by M. Dehn (see **[3]**). Another problem formulated by Dehn (see **[3]**) was the *conjugacy problem*: given arbitrary words w, z from a finite presentation of a group, decide if there is a word x such that w and $x^{-1}zx$ are congruent via the presentation (and thus define conjugate elements in the associated group). It is not difficult to prove that the algorithmic solvability of both the word and conjugacy problems is independent of the fixed finite presentation.

The negative resolution of the above problems represents an important achievement of twentieth century mathematics and one in which both Post and A. A. Markov played a fundamental role. In 1947 Post **[21]** and slightly later Markov **[13]** published independent proofs of the algorithmic unsolvability of the word problem for finitely presented Thue systems. The version of this result stated below reflects contemporary concern with constructive computational methods.

Post-Markov Theorem. *There exists finitely presented Thue systems having algorithmically unsolvable word problem. Moreover, there is an efficient algorithm P which, upon input of any Turing machine $\mathscr{T}$ (resp. normal algorithm $\mathscr{A}$) will output a finitely presented Thue system $P(\mathscr{T})$ (resp. $P(\mathscr{A})$), such that $P(\mathscr{T})$ (resp. $P(\mathscr{A})$) has an algorithmically unsolvable word problem if $\mathscr{T}$ (resp. $\mathscr{A}$) has an algorithmically unsolvable halting problem.*

A brief survey of finitely presented Thue systems with algorithmically unsolvable word problem is given by Matiyasevich **[14]** together with a proof of the Post-Markov Theorem employing normal algorithms. The rewriting techniques developed by Post to represent the computation of a Turing machine find their

way into several textbook proofs of the Novikov-Boone Theorem for the word problem in group theory.

Novikov-Boone Theorem. *There exists finitely presented groups having algorithmically unsolvable word problem. Moreover, there is an efficient algorithm B which upon input of any finitely presented Thue system T will output a finitely presented group* $(B)T$ *such that* $B(T)$ *has algorithmically unsolvable word problem if T has algorithmically unsolvable word problem.*

Examples of presentations of groups with algorithmically unsolvable word problem may be obtained using techniques studied by J. L. Britton (see [**3**]), but at the present time these presentations are quite complicated and involve many defining relators. The situation for finitely presented semigroups is however quite different. The semigroup

$$S = \langle a, b, c, d, e | ac = ca, ad = da, bc = cb, bd = db, eca = ce, edb = de, c^2a = c^2ae \rangle$$

while seeming simple in form has been shown by G. C. Tzeitlin to have an algorithmically unsolvable word problem (see Lallement [**11**] for an accessible proof). It is such striking examples that demonstrate the subtlety of the word problem.

The authors were surprised to discover a relationship between Thue's word problem and Dehn's conjugacy problem. A finitely presented *commutative* Thue system is one whose rewriting rules include (ab, ba) for all distinct a, b in its alphabet. Its associated semigroup is commutative and its word problem is algorithmically solvable. In M. Anshel [**2**] these properties are explicitly employed to show that the conjugacy problem for a special class of finitely presented groups is algorithmically solvable.

Results of a positive nature can be obtained for many large classes of groups and to give a perspective we highlight a few. A group G is termed *residually finite* provided when given $g \in G$, $g \neq 1$, there is a normal subgroup $N_g \lhd G$ such that g is not contained in N_g. Equivalently a group is residually finite if the intersection of the subgroups of finite index is the identity. The word problem for finitely presented residually finite groups is algorithmically solvable since both the words defining the identity element in G and the words defining the nonidentity elements in G are recursively enumerable (see [**3**]).

An important class of groups for which the word problem can be decided is the class of finitely generated groups with a single defining relator (e.g. one relator groups). Dehn originally formulated the word problem in the course of his investigation of the fundamental groups of orientable two dimensional manifolds (which are one relator groups). He did solve the word problem for these groups with the algorithm that has come to be known as *Dehn's algorithm*. Dehn's algorithm is studied geometrically in the context of *small cancellation* groups and more recently has surfaced in the study of *hyperbolic* groups initiated by Gromov (see [**3**]). The complexity of Dehn's algorithm is studied by B. Domanski and M. Anshel in [**6**] where it is shown that a finitely presented group of Dehn's algorithm has word problem solvable in linear time on a deterministic multitape Turing machine. W. Magnus (a student of Dehn) studied the entire class of one relator groups and proved through entirely algebraic means one of the landmark theorems in combinatorial group theory: the word problem for finitely generated one relator groups is algorithmically solvable (see [**3**]). More recently I. Anshel [**1**]

has investigated a class of groups with two relators and at least three generators and again the word problem is seen to be algorithmically solvable. The analysis here is close in spirit to that Magnus employed with the addition of methods from the theory of groups acting on graphs (see [3] for an introduction to these methods). To get some idea of the phenomenon that can arise when looking at this problem the reader is invited to consider the group E given by the presentation

$$\langle a, b \mid a^{-1}b^2a = b^3, b^{-1}a^2b = b^3\rangle$$

and show every word in the generators defines the identity element (i.e. the group is trivial).

Recall that the conjugacy problem requires an algorithm to decide, given two elements in a group, whether or not they are conjugate. A striking result is proved by Charles F. Miller III in [**16**] regarding the conjugacy problem and is very much in the spirit of Post and of Miller's mentor W. W. Boone.

Miller's Theorem. *There exists finitely presented residually finite groups with algorithmically unsolvable conjugacy problem. Moreover, there is an efficient algorithm C which upon input of a finitely presented group G will output a finitely presented residually finite group $C(G)$, such that $C(G)$ has algorithmically unsolvable conjugacy problem if G has algorithmically unsolvable word problem.*

5. PUBLIC-KEY CRYPTOSYSTEMS BASED ON THE WORD AND CONJUGACY PROBLEMS. In conventional cryptography a method is provided to a sender S and a receiver R to transmit messages over an insecure channel by a mechanism such as a *code book* which provides easy encoding and decoding facilities. A particular weakness of such cryptosystems is that an interceptor with knowledge of the encoding facilities can readily decode transmitted messages. Conventional cryptography underwent automation at the end of World War I resulting in the development of mechanical cipher machines. These machines required the possession by both the sender S and the receiver R of a single key k in order to encode and decode a transmitted message. Cryptoanalytic machine attacks (i.e. code-breaking) on one class of cipher machines, the Enigma, provided critical information to the Allies during World War II (see [**8**]–[**10**]).

One response to the advances in codebreaking technology was the introduction of *public-key cryptosystems*. This allows an R to receive messages from many senders $S_1, S_2, \ldots, S_n$ without the introduction of numerous codebooks or keys. These are replaced by a public-key mechanism which enables any sender S_i to easily encode messages which may be then transmitted over insecure channels. The code is designed so that if some third party T intercepts a message, T will find it computationally infeasible to break the code even with knowledge of the encoding mechanism employed by S_i unless the receiver's private key is known to T.

One widely discussed system is the RSA public-key cryptosystem named after its inventors R. L. Rivest, A. Shamir and L. Adelman (see [**22**]). Its security is generally thought to depend on the intractability of factoring large integers. One weakness, common to all public-key cryptosystems is that once the system is specified cryptoanalytic attacks may be initiated. Two such attacks on the RSA system are outlined in [**15**].

Another more ambitious public-key cryptosystem based on the algorithmically unsolvability of the word problem was suggested by N. R. Wagner and M. R.

Magyarik (see [**25**]). Begin with a finitely presented group G specified by,

$$\langle a_1, \ldots, a_n | u_1 = 1, u_2 = 1, \ldots, u_m = 1\rangle$$

with algorithmically unsolvable word problem, together with a *secret homomorphism*

$$h : G \to A$$

to a finitely presented group A with efficiently solvable word problem (such as a large finite group or finitely presented group of Dehn's algorithm). The homomorphism h is specified by its values on the finite generating set of G. Employing a consequence of Von Dyck's theorem [**3**], one can verify that h is a homomorphism by demonstrating that the image of each defining relator of G is the identity in the group A (note that this can be verified since A has efficiently solvable word problem). For this scheme we require two elements of G given respectively by words, y_0, y_1 such that

$$h(y_0) \neq h(y_1).$$

The mechanism for encoding is simply to replace each transmission of a '0' bit by any word y_0' where

$$y_0' = y_0 \bmod G$$

and similarly a '1' bit is replaced by any word y_1', such that $y_1' = y_1 \bmod G$. Thus for example the sequence 0, 1, 1, 0 becomes

$$y_0', y_1', y_1'', y_0''$$

where y_i'' is obtained from y_i' by successively inserting and/or deleting the defining relators of G. In this scheme the group G and the words y_0, y_1 constitute the public-key, while the homomorphism h constitutes the private-key. An interceptor T is faced with solving the word problem for G since R need never reveal the homomorphism $h : G \to A$. Although this system, like any other may be attacked, it is not based on such a fragile mechanism as the intractability of factorization within the current technology.

As a homage to Post we propose a public-key cryptosystem based on Miller's Theorem for constructing finitely presented residually finite groups with algorithmically unsolvable conjugacy problem (this extends the work of N. R. Wagner and M. R. Magyarik). The proposed cryptosystem begins with a finitely presented residually finite group G specified by,

$$\langle a_1, \ldots, a_n; u_1 = e, \ldots, u_k = e\rangle \tag{5.1}$$

with algorithmically unsolvable conjugacy problem (such a group's existence is insured by Miller's theorem, see §4). The additional data required for this system are two elements of $G, \{w, z\}$ such that

$$w \neq 1$$

and

$$z = 1$$

in G. Since G was chosen to be residually finite there exists a finite image of $G, G/N_w$ such that

$$w \notin N_w.$$

Thus when we consider the homomorphism

$$h : G \to G/N_w$$

we may assert that

$$h(w) \neq 1$$
$$h(z) = 1.$$

Hence we conclude that w, z and $h(w), h(z)$ are non-conjugate pairs in G and G/N_w, respectively. We keep the homomorphism h secret and assume that computation in the finite group is efficient enough to determine when two elements specified by words are conjugate or whether a word defines the identity in G/N_w. The mechanism for recoding now follows that of the word problem cryptosystem described above with the enhancement of conjugation by words in G (as well as insertions and deletions of defining relators) being allowed. We observe that the complexity of the word problem for finitely presented residually finite groups is unknown at the time of this writing. In the Kourovka Notebook ([**12**] p. 58), F. B. Cannonito asks:

Do there exist finitely presented residually finite groups with recursive, but not primitive recursive, solution of the word problem?

As with the RSA cryptosystem, the conjugacy problem cryptosystem is based on the computational complexity of a special problem. To date, the research on integer factorization is massive [**18**] as compared to the research on the word problem for residually finite groups. In fact very little is known regarding the computational complexity of the word problem for these groups as the above recursion-theoretic problem indicates.

6. POST'S RELATION TO THE CRYPTOLOGY AND CRYPTOLOGISTS OF HIS ERA. We conclude our discussion by posing the following historical question:

What impact did Post have on the cryptologists of his era?

This question arises from two distinct sources. The first source is the very strong connection between the development of both the theory and practice of digital computation and cryptology and the second concerns Post's contemporaries at the City College of New York, an institution where Post spent nearly his entire adult life.

The intertwining of computation and cryptology is quite explicit in the lives of two individuals, Charles Babbage (1791–1871) and Alan M. Turing (1912–1954). Babbage was a prominent British mathematician whose Difference Engines and Analytic Engines were forerunners of the modern digital computer. He was also prominent among the cryptologists of his era for successful cryptoanalytic attacks on polyalphabetic ciphers (see [**7**]). Turing, a British contemporary of Post, played an instrumental role in the Allied victory in World War II by employing computing machines to break the Enigma code. Turing's life and work are documented in [**9**]. Post was certainly aware and indeed employed Turing's work with regard to the algorithmic unsolvability of the halting problem. It is only natural to ask whether there was a reciprocal interest in Post's work on the part of Turing (from the perspective of cryptology).

It is pointed out in [**7**] that a contemporary of Post, Charles J. Mendelsohn and faculty member of the History Department at the City College was very much involved in cryptological pursuits. In 1918 Mendelsohn was made a Captain in the Military Intelligence Division of the General Staff of the U.S. Army in charge of

decipherment of German codes. Mendelsohn was a classics scholar as well as historian and he pursued a lifelong study of historical ciphers and their originators including a study of Vigenére which appeared in 1940, the year following his death. In fact the proofs of this paper were corrected by his associate and friend, Lt. Col. William F. Friedman, the Prinicpal Cryptoanalyst in the Office of the Chief Signals Officer of the U.S. Army. It was the same Friedman who rebuilt the U.S. cryptoanalytic capability during the 1930's by hiring for the Signals Intelligence Service, Abraham Sinkov and Solomon Kullbeck (both City College graduates and both to go on to doctorates in mathematics and productive cryptological research for the National Security Agency). Friedman is regarded as one of America's top codebreakers in that his work lead to the Japanese defeat at Midway during WWII (see **[10]**).

After discussions with the historian of cryptology David Kahn, and Harold Highland, editor emeritus of the journal *Computers and Security* (who attended City College during the nineteen thirties) there is a clear sense that the informal discussion groups which took place during that period would have lent themselves to consideration of Post's work. Further indications of such contact were evident when, in the course of his address to the November 1988 conference at City College, Marvin Minsky observed that Post rewriting methodology had been employed during the nineteen sixties on a cryptographic project.

The shadowy world of secret intelligence has provided scant information for an historical investigation of these matters. Even such a distinguished mathematician as Peter Hilton reports in **[8]**:

> "I am unfortunately obliged to be reticent about the details of the work we did at Bletchley Park in breaking the highgrade German cipher (sic during WWII). For reasons best known—indeed, almost exclusively known—to themselves, the bureaucrats in Washington and Whitehall steadfastly refuse to declassify such details."

Steven Brams, the noted game theorist and political scientist, has remarked to us that the life and legacy of Emil Post represents one aspect of New York intellectual life during the first half of the twentieth century that is very much in need of deeper exploration. The authors hope that this paper serves to further this pursuit.

The authors would like to thank Martin Davis for supplying us with a preliminary manuscript **[5]** of his biographical and scholarly survey of Post's life and achievements.

REFERENCES

1. I. Anshel, A Freiheitssatz for a class of two-relator groups, *Journal of Pure and Applied Algebra* 72 (1991), 207–250.
2. M. Anshel, The conjugacy problem for *HNN* groups and the word problem for commutative semigroups, *Proc. of the Amer. Math. Soc.*, 61 no. 2 (1976), 223–224.
3. D. E. Cohen, *Combinatorial Group Theory*: *A Topological Approach*, Cambridge University Press, New York (1989).
4. M. Davis, *Computability and Unsolvability*, Dover Publications, Inc., New York (1982).
5. M. Davis, Emil Post: His Life and Work, manuscript.
6. B. Domanski and M. Anshel, The complexity of Dehn's algorithm for word problems in groups, *J. Algorithms* 6 (1985), 543–549.
7. O. I. Franksen, *Mr. Babbage's Secret*: *The Tale of a Cypher- and APL*, Prentice Hall Inc., Englewood Cliffs, New Jersey (1985).

8. P. Hilton, Working with Alan Turing, *The Mathematical Intelligencer* 13, no. 4 (1991), 22–25.
9. A. Hodges, *Alan Turing: The Enigma*, Simon and Schuster, New York (1983).
10. D. Kahn, *The Codebreakers: The Story of Secret Writing*, Macmillan, New York (1967).
11. G. Lallement, *Semigroups and Combinatorial Applications*, John Wiley and Sons, New York (1979).
12. L. J. Leifman and D. J. Johnson trans. ed., *The Kourovka Notebook*, *Unsolved Problems in Group Theory*, AMS trans., series 2, vol. 121 (1983).
13. A. A. Markov, On the impossibility of certain algorithms in the theory of associative systems, I.C.R. (Dokl.) *Acad. Sci. URSS* 55 (1947), 583–586 (English).
14. Yu. V. Matiyasevich, On investigations of some algorithmic problems in algebra and number theory, *Proc. Steklov Inst. Math.*, 168, issue 3, Amer. Math. Soc. Translation (1986), 227–252.
15. K. S. McCurley, Odds and ends from cryptology and computational number theory, in *Cryptology and Computational Number Theory*, C. Pomerance ed., *Proceedings of the Symposia in Applied Math.*, 42, AMS, Providence R.I. (1990), 145–166.
16. C. F. Miller III, *On Group-Theoretic Decision Problems and Their Classification*, Annals Math. Studies, Number 68, Princeton University Press, Princeton, New Jersey (1971).
17. M. L. Minsky, Recursive unsolvability of Post's problem of "tag", and other topics in the theory of Turing machines, *Annals of Math.* 74 (1961), 437–453.
18. C. Pomerance, Factoring, in *Cryptology and Computational Number Theory*, C. Pomerance ed., *Proceedings of the Symposia in Applied Math.*, 42 AMS, Providence, R.I. (1990), 27–47.
19. E. L. Post, Finite combinatory processes—formulation 1, *J. Symbolic Logic* 1, (1936), 103–105.
20. E. L. Post, Recursively enumerable sets of positive integers and their decision problems, *Bull Amer. Math. Soc.* 50 (1944), 284–316.
21. E. L. Post, Recursive unsolvability of a problem of Thue, *J. Symbolic Logic*, 12 (1947), 1–11.
22. R. L. Rivest, A. Shamir and L. Adelman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. of the ACM* (1978), 120–126.
23. A. Thue, Probleme Über Veränderungen von Zeichenreihen nach gegebenen Regeln, *K.V.S.S.* No. **10**, (1914).
24. A. M. Turing, On computable numbers, with an application to the Entscheidungsproblem, *Proc. London Math Soc.* (2) 42 (1936–37), 230–265, A Correction 43 (1937), 544–546.
25. N. R. Wagner and M. R. Magyarik, A public key cryptosystem based on the word problem, in *Advances in Cryptology: Proceedings of Crypto 84*, ed G. R. Blakely and D. Chaum, Lecture Notes in Computer Science, 196 Springer Verlag, New York (1985), 19–36.

Department of Mathematics
Columbia University
New York, NY 10027

Department of Computer Science
The City College, CUNY
New York, NY 10031

There was a professor of Trinity
Who found the square root of infinity;
But in counting the digits
He was seized with the fidgets,
Dropped Science and took to Divinity.

—*American Mathematical Monthly*
28, (1921) p. 394

Famous Nonmathematicians

Steven G. Buyske*

We often tell our students that there are many things besides teaching and actuarial work that they can do with a degree in mathematics, but I don't think they believe us. Over the years I've put together a list of well-known people who were math majors (or some equivalent in other countries and times), although not all of them completed their degrees. It's the most popular thing I've ever had on my office door. When I began this list, it had mostly contemporary Americans, and I called it "People who majored in math." Some of my students added their own names to their copies and posted them on their dorm doors.

I'd be delighted to hear of any additional names.

THE PUBLIC REALM.

Ralph Abernathy, civil rights leader and Martin Luther King's closest aide.

Corazon Aquino, former President of the Philippines. She was a math minor.

Harry Blackmun, Associate Justice of the US Supreme Court, AB *summa cum laude* in mathematics at Harvard.

David Dinkins, Mayor of New York, BA in mathematics from Howard.

Alberto Fujimori, President of Peru, MS in mathematics from the University of Wisconsin-Milwaukee.

Ira Glasser, Executive Director of the American Civil Liberties Union, both a BS and an MA.

Lee Hsien Loong, Deputy Prime Minister of Singapore, a Bachelor's from Cambridge.

Florence Nightingale, pioneer in professional nursing. She was the first person in the English-speaking world to apply statistics to public health. She was also a pioneer in the graphic representation of statistics; the pie-chart was her invention, for example. Not really a math major, she was privately educated, but pursued mathematics far beyond contemporary standards for women.

Paul Painlevé, President of France in the early 20th century, and one of the first passengers of the Wright Brothers. A ringer: he had a distinguished mathematical career.

Carl T. Rowan, columnist for the *Washington Post.*

Laurence H. Tribe, Professor at Harvard Law School, often regarded as one of the great contemporary authorities on Constitutional Law. An AB *summa cum laude* in mathematics from Harvard.

Leon Trotsky, revolutionary. He began to study Pure mathematics at Odessa in 1897, but imprisonment and exile in Siberia seem to have ended his mathematical efforts.

*I'd like to thank my colleagues and the many people on USENET who have given me names and leads.

Eamon de Valera, long-time Prime Minister and then President of the Republic of Ireland. A ringer: he was a mathematics professor before Irish independence.

MUSIC.

Ernst Ansermet, founder and conductor of the Orchestre de la Suisse Romande.

Pierre Boulez, Modernist composer and conductor.

Clifford Brown, Fifties jazz trumpeter.

Art Garfunkel, folk-rock singer. MA in mathematics from Columbia in 1967. Worked on a PhD at Columbia, but chose to pursue his musical career instead.

Phillip Glass, composer, a Bachelor's from the University of Chicago.

Carole King, Sixties songwriter, and later a singer-songwriter. She dropped out after one year of college to pursue her music career.

Tom Lehrer, songwriter-parodist. PhD student in mathematics at Harvard.

Lawrence Leighton Smith, conductor and pianist.

THE OTHER ARTS.

Lewis Carroll, author of *Alice in Wonderland*, *Through the Looking Glass*, and other works. A ringer: he was a logician under his real name, Charles Lutwidge Dodgson.

Heloise (Poncé Cruse Evans), of *Hints from Heloise*. She minored in math.

Larry Niven, science fiction writer, winner of the Nebula and Hugo awards.

Omar Khayyam, author of *The Rubaiyat*. Another ringer: he published works on algebra and Euclid.

Alexander Solzhenitsyn, Nobel prize-winning novelist, a degree in mathematics and physics from the University of Rostov.

Bram Stoker, author of *Dracula*, took honors at Trinity University, Dublin.

Christopher Wren, the architect of St. Paul's Cathedral in London.

FINANCE.

John Maynard Keynes, the great economist. MA and 12th Wrangler, Cambridge University.

J. Pierpont Morgan, the banking, steel, and railroad magnate. Some of the Göttigen faculty tried to convince him to become a professional mathematician.

Ed Thorpe, one of the inventors of program-trading on Wall Street.

PHILOSOPHERS.

Edmund Husserl, the "Father of Phenomenology," PhD 1883 from Vienna.

Ludwig Wittgenstein, one of the giants of twentieth-century philosophy. Studied mathematical logic with Bertrand Russell.

ATHLETES AND OTHER COMPETITORS.

Michael Jordan, basketball superstar. He changed to another major in his junior year.

Davey Johnson, manager of the 1986 New York Mets.

Emanuel Lasker, world chess champion from 1894–1921. Another ringer, he was a mathematics professor with several published papers.

David Robinson, basketball star. BS in mathematics from Annapolis.

Frank Ryan, star quarterback for the Cleveland Browns in the sixties. PhD from Rice.

Virginia Wade, Wimbledon champion, BS in mathematics and physics from Sussex.

LITERARY CRIMINALS.

James Moriarty, former Professor of Mathematics, author of *The Dynamics of an Asteroid*, whose essay on the binomial theorem is said to have had a continental vogue, became the leader of the most sinister criminal conspiracy in Victorian England. He has been called "the Napoleon of Crime." Sherlock Holmes's nemesis.

Mathematics Department
Lafayette College
Easton, PA 18042
buyskes@lafvax.lafayette.edu

PICTURE PUZZLE
(from the collection of Paul Halmos)

The smile came in 1984, soon after his great victory.
(see page 883.)

The Fundamental Theorem of Linear Algebra

Gilbert Strang

This paper is about a theorem and the pictures that go with it. The theorem describes the action of an m by n matrix. The matrix A produces a linear transformation from R^n to R^m—but this picture by itself is too large. The "truth" about $Ax = b$ is expressed in terms of four subspaces (two of R^n and two of R^m). The pictures aim to illustrate the action of A on those subspaces, in a way that students won't forget.

The first step is to see Ax as a *combination of the columns of* A. Until then the multiplication Ax is just numbers. This step raises the viewpoint to subspaces. We see Ax in the ***column space.*** Solving $Ax = b$ means finding all combinations of the columns that produce b in the column space:

$$\underbrace{\begin{bmatrix} | & | & \cdots & | \\ | & | & & | \end{bmatrix}}_{\text{Columns of } A}\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = x_1(\text{column } 1) + \cdots + x_n(\text{column } n) = b.$$

The column space is the range $R(A)$, a subspace of R^m. This abstraction, from entries in A or x or b to the picture based on subspaces, is absolutely essential. Note how subspaces enter *for a purpose*. We could invent vector spaces and construct bases at random. That misses the purpose. Virtually all algorithms and all applications of linear algebra are understood by moving to subspaces.

The key algorithm is elimination. Multiples of rows are subtracted from other rows (and rows are exchanged). There is no change in the ***row space.*** This subspace contains all combinations of the rows of A, which are the columns of A^T. The row space of A is the column space $R(A^T)$.

The other subspace of R^n is the ***nullspace*** $N(A)$. It contains all solutions to $Ax = 0$. Those solutions are not changed by elimination, whose purpose is to compute them. A by-product of elimination is to display the dimensions of these subspaces, which is the first part of the theorem.

The *Fundamental Theorem of Linear Algebra* has as many as four parts. Its presentation often stops with Part 1, but the reader is urged to include Part 2. (That is the only part we will prove—it is too valuable to miss. This is also as far as we go in teaching.) The last two parts, at the end of this paper, sharpen the first two. The complete picture shows the action of A on the four subspaces with the right bases. Those bases come from the singular value decomposition.

The Fundamental Theorem begins with

Part 1. ***The dimensions of the subspaces.***

Part 2. ***The orthogonality of the subspaces.***

The dimensions obey the most important laws of linear algebra:

$$\dim R(A) = \dim R(A^T) \quad \text{and} \quad \dim R(A) + \dim N(A) = n.$$

When the row space has dimension r, the nullspace has dimension $n - r$. Elimination identifies r pivot variables and $n - r$ free variables. Those variables correspond, in the echelon form, to columns with pivots and columns without pivots. They give the dimension count r and $n - r$. Students see this for the echelon matrix and believe it for A.

The *orthogonality* of those spaces is also essential, and very easy. Every x in the nullspace is perpendicular to every row of the matrix, exactly because $Ax = 0$:

$$Ax = \begin{bmatrix} \text{—row} & 1\text{—} \\ \text{—row} & 2\text{—} \\ \text{—row} & m\text{—} \end{bmatrix} x = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

The first zero is the dot product of x with row 1. The last zero is the dot product with row m. One at a time, the rows are perpendicular to any x in the nullspace. So x is perpendicular to all combinations of the rows.

The nullspace $N(A)$ is orthogonal to the row space $R(A^T)$.

What is the fourth subspace? If the matrix A leads to $R(A)$ and $N(A)$, then its transpose must lead to $R(A^T)$ and $N(A^T)$. The fourth subspace is $N(A^T)$, ***the nullspace of*** A^T. We need it! The theory of linear algebra is bound up in the connections between row spaces and column spaces. If $R(A^T)$ is orthogonal to $N(A)$, then—*just by transposing*—the column space $R(A)$ is orthogonal to the "left nullspace" $N(A^T)$. Look at $A^Ty = 0$:

$$A^Ty = \begin{bmatrix} \text{column 1 of } A \\ \vdots \\ \text{column } n \text{ of } A \end{bmatrix} y = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Since y is orthogonal to each column (producing each zero), y is orthogonal to the whole column space. The point is that A^T is just as good a matrix as A. Nothing is new, except A^T is n by m. Therefore the left nullspace has dimension $m - r$.

$A^Ty = 0$ means the same as $y^TA = 0^T$. With the vector on the left, y^TA is a combination of the *rows* of A. Contrast that with $Ax =$ combination of the columns.

The First Picture: Linear Equations

Figure 1 shows how A takes x into the column space. The nullspace goes to the zero vector. Nothing goes elsewhere in the left nullspace—which is waiting its turn.

With b in the column space, $Ax = b$ can be solved. There is a *particular* solution x_r in the row space. The *homogeneous* solutions x_n form the nullspace. The general solution is $x_r + x_n$. The particularity of x_r is that it is orthogonal to every x_n.

May I add a personal note about this figure? Many readers of *Linear Algebra and Its Applications* [4] have seen it as fundamental. It captures so much about $Ax = b$. Some letters suggested other ways to draw the orthogonal subspaces—artistically this is the hardest part. The four subspaces (and very possibly the figure itself) are of course not original. But as a key to the teaching of linear algebra, this illustration is a gold mine.

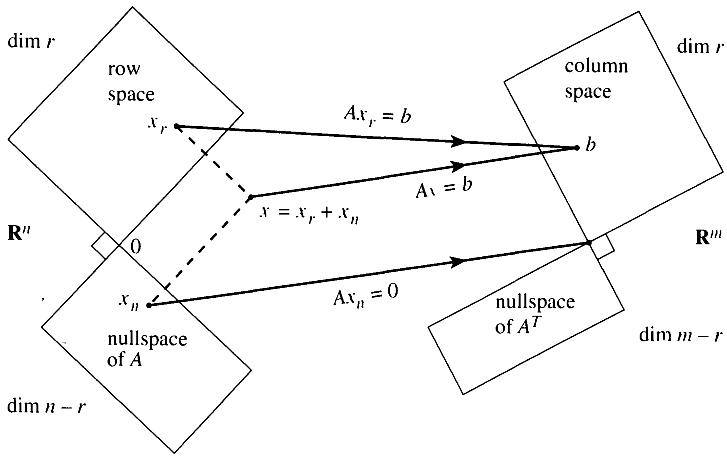


Figure 1. The action of A: Row space to column space, nullspace to zero.

Other writers made a further suggestion. They proposed a lower level textbook, recognizing that the range of students who need linear algebra (and the variety of preparation) is enormous. That new book contains Figures 1 and 2—also Figure 0, to show the dimensions first. The explanation is much more gradual than in this paper—but every course has to study subspaces! We should teach the important ones.

The Second Figure: Least Squares Equations

If b is not in the column space, $Ax = b$ cannot be solved. In practice we still have to come up with a "solution." It is extremely common to have more equations than unknowns—more output data than input controls, more measurements than parameters to describe them. The data may lie close to a straight line $b = C + Dt$. A parabola $C + Dt + Et^2$ would come closer. Whether we use polynomials or sines and cosines or exponentials, the problem is still linear in the coefficients C, D, E:

$$\begin{matrix} C + Dt_1 = b_1 \\ \vdots \\ C + Dt_m = b_m \end{matrix} \qquad \text{or} \qquad \begin{matrix} C + Dt_1 + Et_1^2 = b_1 \\ \vdots \\ C + Dt_m + Et_m^2 = b_m \end{matrix} .$$

There are $n = 2$ or $n = 3$ unknowns, and m is larger. There is no $x = (C, D)$ or $x = (C, D, E)$ that satisfies all m equations. $Ax = b$ has a solution only when the points lie exactly on a line or a parabola—then b is in the column space of the m by 2 or m by 3 matrix A.

The solution is to make the error $b - Ax$ as small as possible. Since Ax can never leave the column space, choose the closest point to b in that subspace. This point is the projection p. Then the error vector $e = b - p$ has minimal length.

To repeat: The best combination $p = A\bar{x}$ is the projection of b onto the column space. The error e is perpendicular to that subspace. Therefore $e = b - A\bar{x}$ is in the left nullspace:

$$A^T(b - A\bar{x}) = 0 \quad \text{or} \quad A^TA\bar{x} = A^Tb.$$

Calculus reaches the same linear equations by minimizing the quadratic $\|b - Ax\|^2$. The chain rule just multiplies both sides of $Ax = b$ by A^T.

The "normal equations" are $A^TA\bar{x} = A^Tb$. They illustrate what is almost invariably true—applications that start with a rectangular A end up computing with the square symmetric matrix A^TA. This matrix is invertible provided A has *independent columns*. We make that assumption: The nullspace of A contains only $x = 0$. (Then $A^TAx = 0$ implies $x^TA^TAx = 0$ which implies $Ax = 0$ which forces $x = 0$, so A^TA is invertible.) The picture for least squares shows the action over on the right side—the splitting of b into $p + e$.

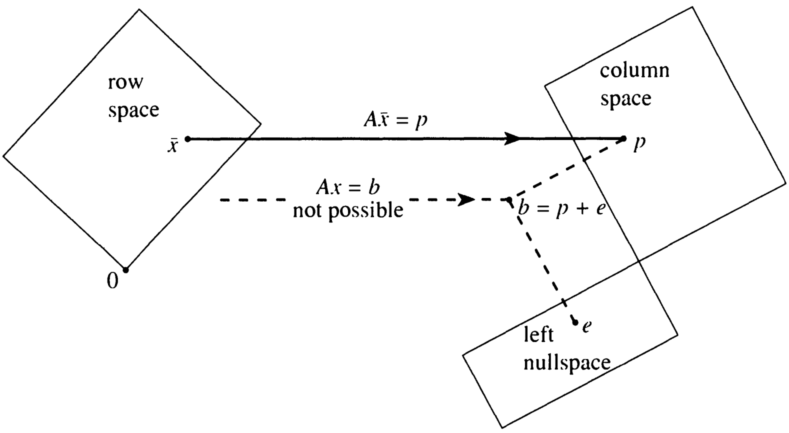


Figure 2. Least squares: $\bar{x}$ minimizes $\|b - Ax\|^2$ by solving $A^TA\bar{x} = A^Tb$.

The Third Figure: Orthogonal Bases

Up to this point, nothing was said about *bases for the four subspaces*. Those bases can be constructed from an echelon form—the output from elimination. This construction is simple, but the bases are not perfect. A really good choice, in fact a "canonical choice" that is close to unique, would achieve much more. To complete the Fundamental Theorem, we make two requirements:

Part 3. ***The basis vectors are orthonormal.***
Part 4. ***The matrix with respect to these bases is diagonal.***

If $v_1, \dots, v_r$ is the basis for the row space and $u_1, \dots, u_r$ is the basis for the column space, then $Av_i = \sigma_i u_i$. That gives a diagonal matrix Σ. We can further ensure that $\sigma_i > 0$.

Orthonormal bases are no problem—the Gram-Schmidt process is available. But a diagonal form involves eigenvalues. In this case they are the eigenvalues of A^TA and AA^T. Those matrices are symmetric and positive semidefinite, so they have nonnegative eigenvalues and orthonormal eigenvectors (which are the bases!). Starting from $A^TAv_i = \sigma_i^2 v_i$, here are the key steps:

$$v_i^TA^TAv_i = \sigma_i^2 v_i^T v_i \quad \text{so that} \quad \|Av_i\| = \sigma_i$$

$$AA^TAv_i = \sigma_i^2 Av_i \quad \text{so that} \quad u_i = Av_i/\sigma_i \text{ is a unit eigenvector of } AA^T.$$

All these matrices have rank r. The r positive eigenvalues σ_i^2 give the diagonal entries σ_i of Σ.

The whole construction is called the *singular value decomposition* (*SVD*). It amounts to a factorization of the original matrix A into $U\Sigma V^T$, where

1. U is an m by m orthogonal matrix. Its columns $u_1, \ldots, u_r, \ldots, u_m$ are basis vectors for the column space and left nullspace.
2. Σ is an m by n diagonal matrix. Its nonzero entries are $\sigma_1 > 0, \ldots, \sigma_r > 0$.
3. V is an n by n orthogonal matrix. Its columns $v_1, \ldots, v_r, \ldots, v_n$ are basis vectors for the row space and nullspace.

The equations $Av_i = \sigma_i u_i$ mean that $AV = U\Sigma$. Then multiplication by V^T gives $A = U\Sigma V^T$.

When A itself is symmetric, its eigenvectors u_i make it diagonal: $A = U\Lambda U^T$. The singular value decomposition extends this spectral theorem to matrices that are not symmetric and not square. The eigenvalues are in Λ, the singular values are in Σ. The factorization $A = U\Sigma V^T$ joins $A = LU$ (elimination) and $A = QR$ (orthogonalization) as a beautifully direct statement of a central theorem in linear algebra.

The history of the *SVD* is cloudy, beginning with Beltrami and Jordan in the 1870's, but its importance is clear. For a very quick history and proof, and much more about its uses, please see [**1**]. "The most recurring theme in the book is the practical and theoretical value of this matrix decomposition." The *SVD* in linear algebra corresponds to the Cartan decomposition in Lie theory [**3**]. This is one more case, if further convincing is necessary, in which mathematics gets the properties right—and the applications follow.

Example

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix} = \frac{\begin{bmatrix} 1 & -3 \\ 3 & 1 \end{bmatrix}}{\sqrt{10}} \begin{bmatrix} \sqrt{50} & 0 \\ 0 & 0 \end{bmatrix} \frac{\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}}{\sqrt{5}} = U\Sigma V^T.$$

All four subspaces are 1-dimensional. The columns of A are multiples of $\begin{bmatrix} 1 \\ 3 \end{bmatrix}$ in U. The rows are multiples of $[1 \quad 2]$ in V^T. Both A^TA and AA^T have eigenvalues 50 and 0. So the only singular value is $\sigma_1 = \sqrt{50}$.

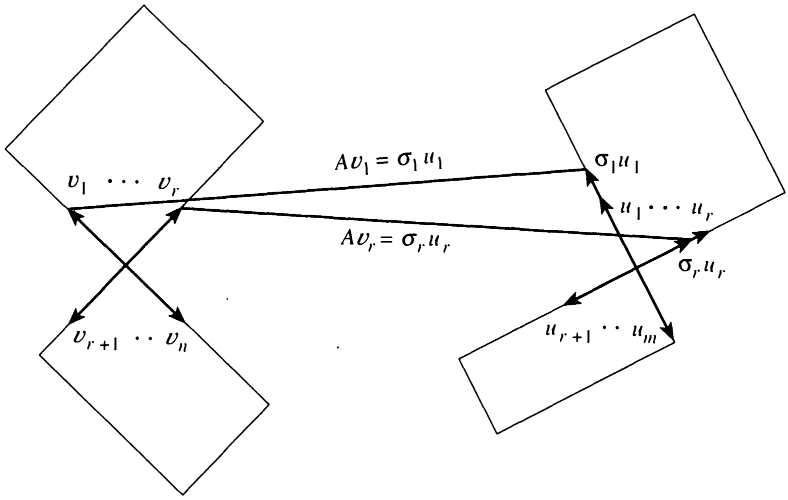


Figure 3. Orthonormal bases that diagonalize A.

The *SVD* expresses A as a combination of r rank-one matrices:

$$A = U\Sigma V^T = u_1\sigma_1 v_1^T + \cdots + u_r\sigma_r v_r^T \qquad \left(\text{here } A = \begin{bmatrix} 1 \\ 3 \end{bmatrix}\begin{bmatrix} 1 & 2 \end{bmatrix}\right).$$

The Fourth Figure: The Pseudoinverse

The *SVD* leads directly to the "*pseudoinverse*" of A. This is needed, just as the least squares solution $\bar{x}$ was needed, to invert A and solve $Ax = b$ when those steps are strictly speaking impossible. The pseudoinverse A^+ agrees with A^{-1} when A is invertible. The least squares solution of minimum length (having no nullspace component) is $x^+ = A^+b$. It coincides with $\bar{x}$ when A has full column rank $r = n$—then A^TA is invertible and Figure 4 becomes Figure 2.

A^+ takes the column space back to the row space [4]. On these spaces of equal dimension r, the matrix A is invertible and A^+ inverts it. On the left nullspace, A^+ is zero. I hope you will feel, after looking at Figure 4, that this is the one natural best definition of an inverse. Despite those good adjectives, the *SVD* and A^+ is too much for an introductory linear algebra course. It belongs in a second course. Still the picture with the four subspaces is absolutely intuitive.

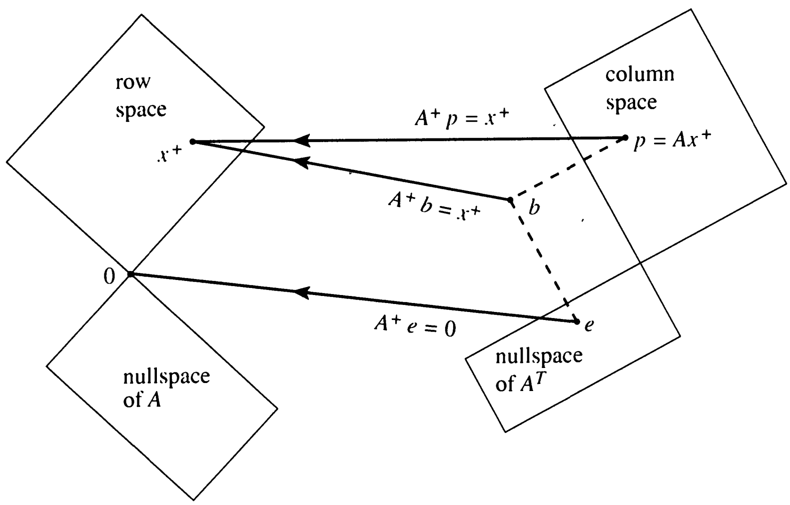


Figure 4. The inverse of A (where possible) is the pseudoinverse A^+.

The *SVD* gives an easy formula for A^+, because it chooses the right bases. Since $Av_i = \sigma_i u_i$, the inverse has to be $A^+u_i = v_i/\sigma_i$. Thus the pseudoinverse of Σ contains the reciprocals $1/\sigma_i$. The orthogonal matrices U and V^T are inverted by U^T and V. All together, *the pseudoinverse of* $A = U\Sigma V^T$ *is* $A^+ = V\Sigma^+U^T$.

Example (continued)

$$A^+ = \frac{\begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}}{\sqrt{5}} \begin{bmatrix} 1/\sqrt{50} & 0 \\ 0 & 0 \end{bmatrix} \frac{\begin{bmatrix} 1 & 3 \\ -3 & 1 \end{bmatrix}}{\sqrt{10}} = \frac{1}{50}\begin{bmatrix} 1 & 3 \\ 2 & 6 \end{bmatrix}.$$

Always A^+A is the identity matrix on the row space, and zero on the nullspace:

$$A^+A = \frac{1}{50}\begin{bmatrix} 10 & 20 \\ 20 & 40 \end{bmatrix} = \text{projection onto the line through } \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

Similarly AA^+ is the identity on the column space, and zero on the left nullspace:

$$AA^+ = \frac{1}{50}\begin{bmatrix} 5 & 15 \\ 15 & 45 \end{bmatrix} = \text{projection onto the line through } \begin{bmatrix} 1 \\ 3 \end{bmatrix}.$$

A Summary of the Key Ideas

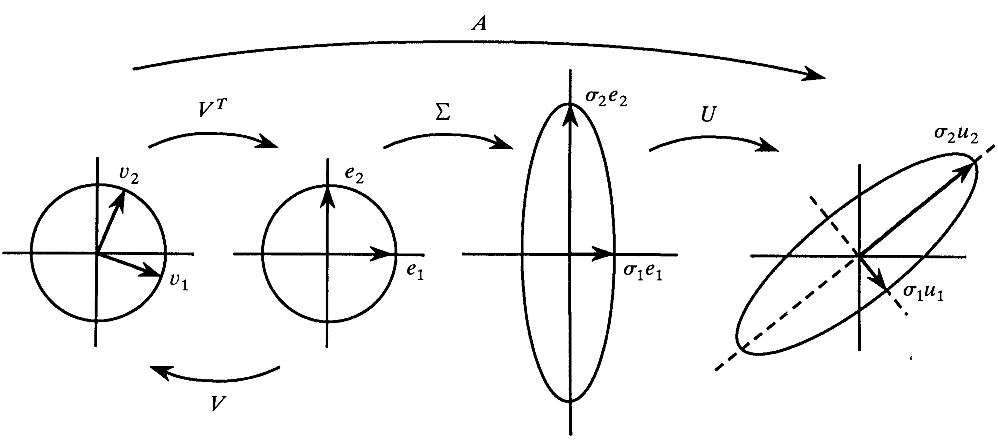
From its r-dimensional row space to its r-dimensional column space, A yields an invertible linear transformation.

Proof: Suppose x and x' are in the row space, and Ax equals Ax' in the column space. Then $x - x'$ is in both the row space and nullspace. It is perpendicular to itself. Therefore $x = x'$ and the transformation is one-to-one.

The SVD chooses good bases for those subspaces. Compare with the Jordan form for a real square matrix. There we are choosing the *same basis* for both domain and range—our hands are tied. The best we can do is $SAS^{-1} = J$ or $SA = JS$. In general J is not real. If real, then in general it is not diagonal. If diagonal, then in general S is not orthogonal. By choosing *two bases*, not one, every matrix does as well as a symmetric matrix. The bases are orthonormal and A is diagonalized.

Some applications permit two bases and others don't. For powers A^n we need S^{-1} to cancel S. Only a similarity is allowed (one basis). In a differential equation $u' = Au$, we can make one change of variable $u = Sv$. Then $v' = S^{-1}ASv$. But for $Ax = b$, the domain and range are philosophically "not the same space." The row and column spaces are isomorphic, but their bases can be different. And for least squares the *SVD* is perfect.

This figure by Tom Hern and Cliff Long [**2**] shows the diagonalization of A. Basis vectors go to basis vectors (principal axes). A circle goes to an ellipse. The matrix is factored into $U\Sigma V^T$. Behind the scenes are *two* symmetric matrices A^TA and AA^T. So we reach two orthogonal matrices U and V.



We close by summarizing the action of A and A^T and A^+:

$$Av_i = \sigma_i u_i \qquad A^T u_i = \sigma_i v_i \qquad A^+ u_i = v_i/\sigma_i \qquad 1 \leqslant i \leqslant r.$$

The nullspaces go to zero. Linearity does the rest.

The support of the National Science Foundation (DMS 90-06220) is gratefully acknowledged.

REFERENCES

1. Gene Golub and Charles Van Loan, *Matrix Computations*, 2nd ed., Johns Hopkins University Press (1989).
2. Thomas Hern and Cliff Long, Viewing some concepts and applications in linear algebra, *Visualization in Teaching and Learning Mathematics*, MAA Notes 19 (1991) 173–190.
3. Roger Howe, Very basic Lie theory, *American Mathematical Monthly*, 90 (1983) 600–623.
4. Gilbert Strang, *Linear Algebra and Its Applications*, 3rd ed., Harcourt Brace Jovanovich (1988).
5. Gilbert Strang, *Introduction to Linear Algebra*, Wellesley-Cambridge Press (1993).

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139
gs@math.mit.edu

An Identity of Daubechies

The generalization of an identity of Daubechies using a probabilistic interpretation by D. Zeilberger [100 (1993) 487], has already appeared in SIAM Review Problem 85-10 (June, 1985) in a slightly more general context. In addition to a similar probabilistic derivation there is also a direct algebraic proof. Incidentally, problem 10223 [99 (1992) 462] is the same as the identity of Daubechies and a slight generalization of this identity has appeared previously as problem 183, Crux Math. 3(1977) 69–70 and came from a list of problems considered for the Canadian Mathematical Olympiad. There was an inductive solution of the latter by Mark Kleinman, a high school student at the time and one of the top students in the U.S.A.M.O. and the I.M.O.

M. S. Klamkin
Department of Mathematics
University of Alberta
Edmonton, Alberta
CANADA T6G 2G1

A Simple Proof of the Jordan-Alexander Complement Theorem

Albrecht Dold

The complements of homeomorphic subsets $A, B \subset \mathbb{R}^n$ of Euclidean space need not be homeomorphic, $A \approx B \not\Rightarrow (\mathbb{R}^n - A) \approx (\mathbb{R}^n - B)$. This is well illustrated by classical knot theory, i.e. when A, B are knots in $\mathbb{R}^3$. The complements usually have different fundamental groups in this case, $\pi_1(\mathbb{R}^3 - A) \not\cong \pi_1(\mathbb{R}^3 - B)$, and this fundamental group serves to distinguish non-equivalent knots.

On the other hand, it is a classical consequence of **Alexander** duality (cf. **[D]**, VIII, 8.15) that the homology groups of the complements agree if A, B are homeomorphic closed subsets of $\mathbb{R}^n$. Thus,

Theorem. *If $A, B \subset \mathbb{R}^n$ are homeomorphic closed subsets then their complements have isomorphic homology groups, $H(\mathbb{R}^n - A) \cong H(\mathbb{R}^n - B)$,—also in generalised (co-)homology.*

If the coefficients of homology are taken in a commutative ring R with 1 then the rank of $H_0(\mathbb{R}^n - A)$ equals the number of components of $\mathbb{R}^n - A$ (almost by definition of H_0). Therefore,

Corollary. *The complements of homeomorphic closed subsets $A, B \subset \mathbb{R}^n$ have the same number of components.*

If $A = \{x \in \mathbb{R}^n | \, \|x\| = 1\} = S^{n-1}$, the **Jordan** separation theorem is: Every subset $B \subset \mathbb{R}^n$, $n > 1$, which is homeomorphic to S^{n-1} separates $\mathbb{R}^n$ into two regions.

In this note we give a simple proof of the theorem. It uses basic properties only of homology, namely homotopy invariance and Mayer-Vietoris sequences of open subsets of Euclidean spaces. The reader might take singular or simplicial homology but the proof also works in general (co-)homology—no dimension axiom is required. No priority is claimed for this note. Its methods are familiar in topology and algebraic geometry; the intention is to publicize an elegant argument.

It is convenient to use reduced homology in the proof. The *reduced homology* $\tilde{H}X$ of a non-empty space X is the kernel of the homomorphism $HX \to HP$ which is induced by the map $X \to P$ onto the one-point space P. If we choose a point in X, which we write as a map $P \to X$, then the composition $P \to X \to P$ is the identity map, hence $HX = \mathrm{im}(HP \to HX) \oplus \ker(HX \to HP) = HP \oplus \tilde{H}X$. Thus, HX differs from $\tilde{H}X$ by the constant summand HP only. In particular, $\tilde{H}P = 0$ and by homotopy invariance, $\tilde{H}X = 0$ for every contractible space X.

Proposition 1. *For every closed subset $A \subset \mathbb{R}^n$, $A \neq \mathbb{R}^n$, we have $\tilde{H}_i(\mathbb{R}^n - A) \cong \tilde{H}_{i+1}(\mathbb{R}^{n+1} - A)$, where $\mathbb{R}^{n+1} = \mathbb{R}^n \times \mathbb{R}$, $\mathbb{R}^n = \mathbb{R}^n \times \{0\} \subset \mathbb{R}^{n+1}$.*

Proof: Put $Z = \mathbb{R}^{n+1} - A$,

$$Z_+ = \{(x,t) \in \mathbb{R}^n \times \mathbb{R} | t > 0, \text{ or } x \in (\mathbb{R}^n - A)\},$$
$$Z_- = \{(x,t) \in \mathbb{R}^{n+1} | t < 0 \text{ or } x \in (\mathbb{R}^n - A)\}.$$

Then Z_+, Z_- are open in Z,

$$Z_+ \cup Z_+ = Z, Z_+ \cap Z_- = (\mathbb{R}^n - A) \times \mathbb{R}.$$

Furthermore, Z_+ and Z_- are contractible (the deformation $(x,t) \mapsto (x, (1-\tau)t + \tau)$, $0 \leq \tau \leq 1$, moves Z_+ into the hyperplane $t = 1$ which in turn deforms into a point), hence $\tilde{H}(Z_+) = 0 = \tilde{H}(Z_-)$. The reduced Mayer-Vietoris sequence (which is the ordinary Mayer-Vietoris sequence without the superfluous constant summands HP; cf. **[D]**, III, 8.15) has the form

$$\tilde{H}_{i+1}(Z_+) \oplus \tilde{H}_{i+1}(Z_-) \to \tilde{H}_{i+1}(Z_+ \cup Z_-) \to \tilde{H}_i(Z_+ \cap Z_-)$$
$$\to \tilde{H}_i(Z_+) \oplus \tilde{H}_i(Z_-).$$

As it is exact and $\tilde{H}(Z_+) = 0 = \tilde{H}(Z_-)$ it amounts to an isomorphism $\tilde{H}_{i+1}(Z_+ \cup Z_-) \cong \tilde{H}_i(Z_+ \cap Z_-)$. But $Z_+ \cup Z_- = \mathbb{R}^{n+1} - A$, and $Z_+ \cap Z_- = (\mathbb{R}^n - A) \times \mathbb{R}$; the latter deforms into $(\mathbb{R}^n - A) \times \{0\} = \mathbb{R}^n - A$. ■

Iterating Propostion 1 we get

Proposition 2. *For every closed subset $A \subset \mathbb{R}^n$, $A \neq \mathbb{R}^n$, and every $q \geq 0$, $\tilde{H}_{i+q}(\mathbb{R}^{n+q} - A) \cong \tilde{H}_i(\mathbb{R}^n - A)$.* ■

Proposition 3. *If $A \subset \mathbb{R}^p$, $B \subset \mathbb{R}^q$ are closed subsets which are homeomorphic then the complements of $A = A \times \{0\}$ and $B = \{0\} \times B$ in $\mathbb{R}^{p+q} = \mathbb{R}^p \times \mathbb{R}^q$ are also homeomorphic*, $(\mathbb{R}^{p+q} - A) \approx (\mathbb{R}^{p+q} - B)$.

Proof: (Compare **[FM]**, §3). Let $\varphi: A \rightleftarrows B: \psi$ be reciprocal homeomorphisms, $\psi\varphi = 1_A$, $\varphi\psi = 1_B$. By Tietze's Lemma, these extend to continuous maps $\Phi: \mathbb{R}^p \rightleftarrows \mathbb{R}^q: \Psi$. The maps $L, R: \mathbb{R}^p \times \mathbb{R}^q \to \mathbb{R}^p \times \mathbb{R}^q$, $L((x,y) = (x, y - \Phi(x)$, $R(x,y) = (x - \Psi(y), y)$ are self-homeomorphisms of $\mathbb{R}^{p+q}$, and they map the graph $\Gamma = \{(x,y) \in \mathbb{R}^p \times \mathbb{R}^q | x \in A, y = \varphi(x)\} = \{(x,y) | y \in B, x = \psi(y)\}$ onto A resp. B. Hence $(\mathbb{R}^{p+q} - A) \overset{L}{\approx} (\mathbb{R}^{p+1} - \Gamma) \overset{R}{\approx} (\mathbb{R}^{p+q} - B)$. ■

Proof of the theorem. If both A and B are $\neq \mathbb{R}^n$ we apply propositions 2, 3, 2 in this order, $\tilde{H}_i(\mathbb{R}^n - A) \cong \tilde{H}_{i+n}(\mathbb{R}^{n+n} - A) \cong \tilde{H}_{i+n}(\mathbb{R}^{n+n} - B) \cong \tilde{H}_i(\mathbb{R}^n - B)$. Adding $H_i P$ to both ends gives $H_i(\mathbb{R}^n - A) \cong H_i(\mathbb{R}^n - B)$, as required.

If $A = \mathbb{R}^n$ we still have $\tilde{H}_j(\mathbb{R}^{n+1} - A) \cong \tilde{H}_j(\mathbb{R}^{n+1} - B)$ by the same argument; in particular, $\tilde{H}_0(\mathbb{R}^{n+1} - A) \cong \tilde{H}_0(\mathbb{R}^{n+1} - B)$. But $\mathbb{R}^{n+1} - A = \mathbb{R}^{n+1} - \mathbb{R}^n$ has two components and $\mathbb{R}^{n+1} - B$ has only one component—unless $B = \mathbb{R}^n$. Therefore, (in ordinary homology), rank $(\tilde{H}_0(\mathbb{R}^{n+1} - A)) = 1$ and rank $(\tilde{H}_0(\mathbb{R}^{n+1} - B)) = 0$—unless $B = \mathbb{R}^n$. Therefore, $B = \mathbb{R}^n = A$. ■

REFERENCES

[D] Dold, A., Lectures on Algebraic Topology. Springer Verlag Berlin-Heidelberg-New York, 1972/80.

[FM] Fulton, W., MacPherson, R., Categorial Framework for the Study of Singular Spaces. Mem. Amer. Math. Soc. 243 (1981).

Mathematisches Institut
Im Neuenheimer Feld 288
D-69120 Heidelberg 1
Germany

Squaring the Circle with Holes

Hansklaus Rummler

1. WALLIS' PRODUCT. Among the approximations of π, Wallis' product

$$\frac{\pi}{2} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdots$$

is perhaps the most fascinating one. Sure, it is not really useful in calculating π, the product converging very slowly. But the formula is already interesting for its history: Wallis' somewhat mysterious—or even mystic—discovery of the formula inspired Newton to similar calculations, leading finally to the binomial series (see [1]).

Nowadays, the proof of Wallis' formula has become a standard exercise: Calculating the integral

$$I_m = \int_0^{\pi/2} \sin^m x \, dx$$

for every natural number m leads to

$$I_{2n} = \frac{\pi}{2} \cdot \frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} \quad \text{and} \quad I_{2n+1} = \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdots \frac{2n}{2n+1},$$

and from this Wallis' product formula is easily derived.

An alternative proof is obtained by taking $z = \frac{1}{2}$ in the Weierstraß product

$$\sin(\pi z) = \pi z \prod_{\nu=1}^{\infty} \left(1 - \frac{z^2}{\nu^2}\right).$$

Unfortunately, neither proof helps to understand the formula. To explain what we mean by *understanding a formula*, let us consider Vieta's formula:

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}} + \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}} \cdot \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}}$$

$$\cdot \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}}} \cdots .$$

The factors of this infinite product are much more complicated than those of Wallis' product, but they have a simple geometric meaning, because they represent length ratios: If l_n denotes the length of a regular 2^n-gon inscribed in the unit circle, it can be shown that the factors of Vieta's product are just the ratios

$l_n : l_{n+1}$, and the formula is immediately clear:

$$\frac{2}{\pi} = \frac{l_1}{l_\infty} = \lim_{n\to\infty} \frac{l_1}{l_2} \cdot \frac{l_2}{l_3} \cdots \frac{l_n}{l_{n+1}} = \frac{l_1}{l_2} \cdot \frac{l_2}{l_3} \cdot \frac{l_3}{l_4} \cdot \frac{l_4}{l_5} \cdots$$

(The inscribed 2-gon is a diameter, counted twice.)

2. WALLIS' SIEVE. Instead of trying to *understand* Wallis' product formula in the same sense we understand Vieta's formula, we shall *interpret* it, constructing a subset of the unit square that is easily seen to have area $\frac{8}{9} \cdot \frac{24}{25} \cdot \frac{48}{49} \cdots$, which, by Wallis' product formula, is just the area of the inscribed disk, namely $\pi/4$.

In order to construct this set, let us say that we *punch a hole of order n* into a square, n being an odd integer, if we take away the middle open one of the n^2 congruent small squares into which we can decompose the given square.

Now take a compact unit square and punch a hole of order 3 into this square. The remaining set W_1 has of course area

$$\mu(W_1) = \frac{8}{9}.$$

Punching a hole of order 5 into each of the 8 small squares forming W_1, we get a set W_2 consisting of $8 \cdot 24$ small squares and with area

$$\mu(W_2) = \frac{8}{9} \cdot \frac{24}{25}.$$

Continuing in this way by punching holes of order 7, 9, 11 and so on, we get finally *Wallis's sieve*, a compact set W_∞ with area

$$\mu(W_\infty) = \frac{8}{9} \cdot \frac{24}{25} \cdot \frac{48}{49} \cdots = \frac{\pi}{4}.$$

The following figures show the first three steps of our construction:

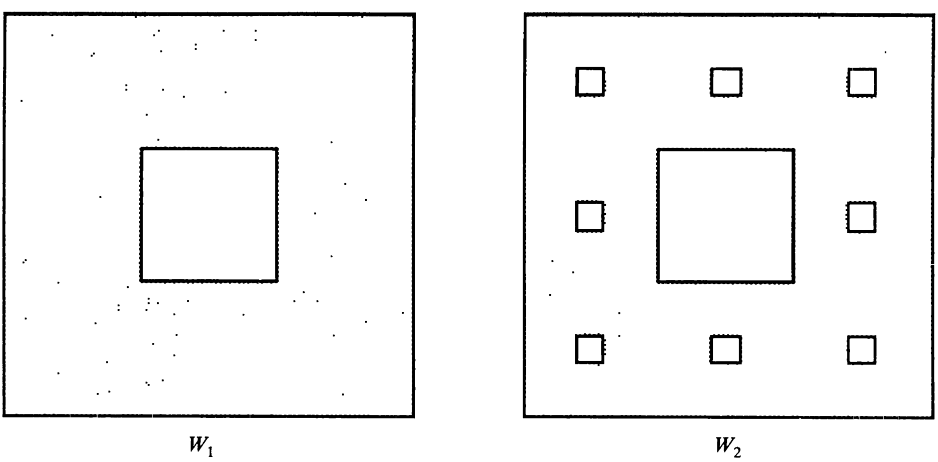
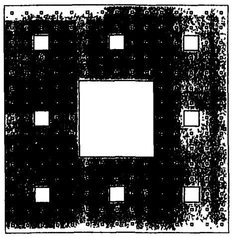


Figure 1



W_3

Figure 2

3. WALLIS' SIEVE AND LEBESGUE MEASURE. So far, there seems to be no problem in calculating the area of Wallis' sieve W_∞, and by construction this area is just $\mu(W_\infty) = \frac{8}{9} \cdot \frac{24}{25} \cdot \frac{48}{49} \cdots = \pi/4$. But we have to be careful: *area* here means *Lebesgue measure*, because W_∞ is not measurable in Jordan's sense, its interior measure being 0. W_∞ does not even contain any product set $A \times B$ with $A, B \subset \mathbb{R}$ having positive Lebesgue measure. To see this, consider a maximal product subset of W_1, for instance $[0,1] \times ([0, \frac{1}{3}] \cup [\frac{2}{3}, 1])$. This subset has measure $\frac{2}{3}$, a maximal product subset of W_2 has measure $\frac{2}{3} \cdot \frac{4}{5}$, and so on. Therefore, a maximal product subset of W_∞ has measure $\frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdots = 0$.

Thus, Wallis' sieve W_∞ is an example of a subset of the plane $\mathbb{R}^2$ with positive Lebesgue measure, but not admitting any product subset with positive Lebesgue measure.

REFERENCE

1. C. H. Edwards, Jr., *The Historical Development of the Calculus*, Springer-Verlag, New York, 1979, pp. 166–176.

Institut de Mathématiques
de l'Université de Fribourg,
Chemin du Musée 23,
CH-1700 FRIBOURG

Fermat's Last Problem

An Englishman named Wiles discovered the key,
To Fermat's Last Problem using geometry.
By proving the sum of two powers,
Is a number to the power.
If and only if the power is smaller than three.

—Nats Wolraf

Simplifying the Proof of Dirichlet's Theorem

Paul Monsky

Dirichlet showed that an arithmetic progression $a, a + D, a + 2D, \ldots$ with $D \geqslant 1$ and $(a, D) = 1$ contains infinitely many primes. Most of his argument is accessible to undergraduate mathematics majors, but a proof of the theorem is seldom presented to them because of the reputed difficulty of a key step—showing that certain infinite sums are non-zero. This note outlines a simple proof of the non-vanishing of these sums. The argument is very close to one given by Gelfond, [**1**], but is easier and works well in the classroom.

The sums I'll treat may be described as follows. A "character to the modulus D" is a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ satisfying:

(1) If $a \equiv b(D)$, then $\chi(a) = \chi(b)$
(2) $\chi(ab) = \chi(a)\chi(b)$
(3) $\chi(a) = 0$ if and only if $(a, D) > 1$.

χ is said to be *real* if it takes real values (which can only be 1, -1, or 0), *non-principal* if it takes values other than 0 or 1. Suppose for example that D is an odd prime. Then the "Legendre symbol", taking each quadratic residue of D to 1, each non-residue to -1 and each multiple of D to 0 is a real non-principal character. For a non-principal χ, $\Sigma_1^\infty \chi(n)/n$ converges. (This follows from summation by parts; see the argument given in the last paragraph of this note.)

The usual approach to proving Dirichlet's theorem involves several standard analytic techniques (see [**2**], for example); the main non-formal step is showing that $\Sigma_1^\infty \chi(n)/n \neq 0$ whenever χ is real and non-principal (the result is also needed for non-real χ, but this is fairly easily handled). Dirichlet's original non-vanishing proof involved a detour through the theory of binary quadratic forms. Modern proofs generally use ideal theory in quadratic number fields or some complex variable theory. Elementary proofs are also known, but are more complicated than the one I'll now present.

One begins by defining c_n to be $\Sigma\chi(d)$ where d ranges over the positive divisors of n. Evidently $c_{p^a} = 1 + \chi(p) + \chi(p)^2 + \cdots + \chi(p)^a \geqslant 0$. It follows easily that $c_n \geqslant 0$ for all n. Furthermore, $c_n = 1$ whenever n is a power of a prime p dividing D. In particular $\Sigma_1^\infty c_n = \infty$.

Next, following [**1**], one sets $f(t) = \Sigma_1^\infty \chi(n)t^n/(1 - t^n)$. The series evidently converges in $[0, 1)$. Expanding each $t^n/(1 - t^n)$ one finds that $f(t) = \Sigma_1^\infty c_n t^n$. The paragraph above shows that $f(t) \to \infty$ as $t \to 1^-$. Suppose now that $\Sigma_1^\infty \chi(n)/n = 0$. Then $-f(t) = \Sigma_1^\infty \chi(n)[\{1/n(1 - t)\} - \{t^n/(1 - t^n)\}]$; write this as $\Sigma_1^\infty \chi(n)b_n$.

The critical observation is that $b_1 \geqslant b_2 \geqslant b_3 \geqslant \cdots$. Note first that

$$\begin{aligned}(1 - t)(b_n - b_{n+1}) &= \frac{1}{n} - \frac{1}{n+1} - \frac{t^n}{1 + t + \cdots + t^{n-1}} + \frac{t^{n+1}}{1 + t + \cdots + t^n} \\ &= \frac{1}{n(n+1)} - \frac{t^n}{(1 + t + \cdots + t^{n-1})(1 + t + \cdots + t^n)}.\end{aligned}$$

Since $(1 + t + \cdots + t^{n-1}) \geqslant nt^{(n-1)/2} \geqslant nt^{n/2}$ while $(1 + t + \cdots + t^n) \geqslant (n + 1)t^{n/2}$ (this is the inequality of the arithmetic and geometric mean), $b_n - b_{n+1} \geqslant 0$.

Now χ is periodic of period D, and $\sum_1^D \chi(n) = 0$. So the numbers $\chi(1), \chi(1) + \chi(2), \chi(1) + \chi(2) + \chi(3), \ldots$ are bounded in absolute value by D. Since $b_n \searrow 0$, the standard Abel rearrangement of the infinite sum $\sum_1^\infty \chi(n) b_n$ shows that $|\sum_1^\infty \chi(n) b_n| \leqslant Db_1 = D$, contradicting the unboundedness of f on $[0, 1)$.

REFERENCES

1. A. O. Gelfond, *Elementary Methods in Analytic Number Theory*, Rand McNally and Co, 1965, pp. 47–49.
2. H. Davenport, *Multiplicative Number Theory*, Markham, Chicago, 1967.

Department of Mathematics
Brandeis University
Waltham, MA 02254-9110

Why is P^2 Not Embeddable in R^3?

Hiroshi Maehara

The projective plane P^2 is the closed surface obtained by pasting a Möbius band and a 2-cell together along their boundaries. The surface P^2 is not embeddable in the 3-dimensional Euclidean space R^3. Though this fact is well known, no handy proof seems to be furnished yet. (A proof in Spanier [3], for instance, requires cohomology theory.) Here, we offer a short and clear-cut proof of the non-embeddability of P^2 in R^3 by applying the *Link Appearing Theorem*.

Our figures in R^3 are assumed to be *tame*. (A figure X in R^3 is tame if there exists a homeomorphism f: $R^3 \to R^3$ such that $f(X)$ is a polygonal or polyhedral figure.) Thus, we consider only tame embeddings. A (2-component) *link* is an embedding of a pair of circles in R^3. Let us call a link *trivial* if one of the two

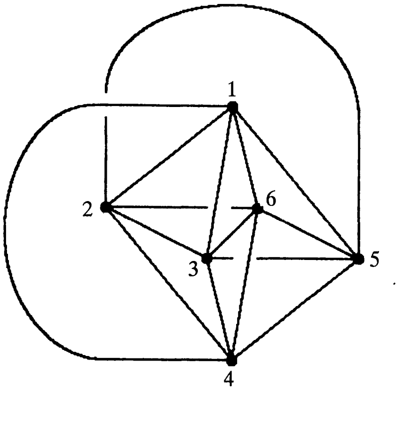


Figure 1.

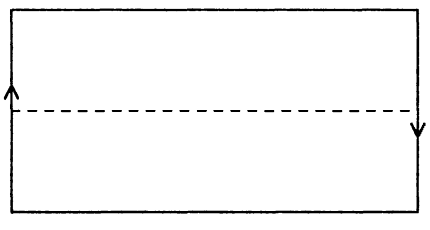


Figure 2.

curves bounds a 2-cell in R^3 that is disjoint from the other curve. Otherwise, it is *non-trivial*.

Now, consider a set of six points in R^3, and assume that each pair of these points is connected by a simple curve such that the curves meet only at their endpoints. Such a figure is called a *complete 6-graph* and is usually denoted K_6. Fig. 1 shows a K_6 in which six points are indicated by $1, 2, \ldots, 6$. A simple closed curve in a K_6 is called a *cycle* of the K_6. We indicate a cycle by a sequence of points in the order of appearing when we trace the cycle. In the K_6 of Fig. 1, the pair of cycles 135 and 246 forms a non-trivial link.

Link Appearing Theorem. *Any complete* 6-*graph in* R^3 *contains a pair of disjoint cycles that forms a non-trivial link.* ■

This theorem was proved by Sachs **[2]** and independently by Conway-Gordon **[1]**. Its proof is not difficult, see **[1]** or **[2]** for the detail.

In a rectangular representation of a Möbius band M, the line segment connecting the midpoints of the to-be-identified sides (the dotted line in Fig. 2) represents a simple closed curve in the Möbius band M. This closed curve is called the *meridian* of M.

Lemma. *For any embedding of a Möbius band M in R^3, the pair $(\partial M, C)$ of the boundary ∂M and the meridian C of M forms a non-trivial link.*

Proof: Consider the K_6 on the Möbius band M represented in Fig. 3. (Each pair of the six points $1, 2, \ldots, 6$ is, indeed, connected by a simple curve. For example, the line segment from the point 1 to the right-top e and the line segment from the left-bottom e to the point 3 make together a simple curve connecting 1 and 3.) This K_6 contains ten pairs of disjoint cycles:

$$(123, \underline{456}), (\underline{124}, 356), (125, \underline{346}), (\underline{126}, 345), (134, 256),$$

$$(\underline{135}, 246), (136, \underline{245}), (145, \underline{236}), (146, \underline{235}), (\underline{156}, 234).$$

Each underlined cycle bounds a 2-cell in M that is disjoint from its partner cycle. For example, the cycle 135 bounds the 2-cell shaded in Fig. 3. Hence, in any embedding of the Möbius band M in R^3, nine pairs of cycles of K_6 other than $(134, 256)$ are trivial links. Therefore, $(134, 256)$ must be a non-trivial link by the Link Appearing Theorem. The cycle 256 is the meridian of M, and the cycle 134 is the boundary ∂M. ■

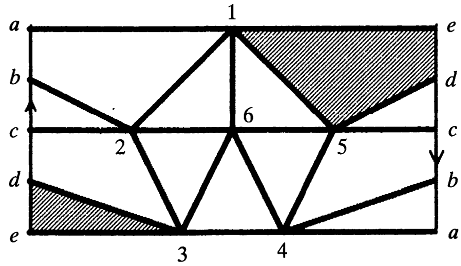


Figure 3.

Proof of the non-embeddability of P^2 in R^3. Suppose P^2 is embedded in R^3. By removing an open 2-cell D from the surface P^2, we have a Möbius band M. Then, the boundary ∂M and the meridian C of M form together a non-trivial link. Therefore, C and the 2-cell D must intersect each other, a contradiction. ∎

REFERENCES

1. J. H. Conway and C. McA. Gordon, Knots and links in spatial graphs, *J. Graph Theory*, 7 (1985), 445–452.
2. H. Sachs, On a spatial analogue of Kuratowski's theorem on planar graphs—an open problem, in *Graph Theory*, Lagow 1981, Lecture Note in Math. #1018, Springer Verlag, Berlin, 1982, 230–241.
3. E. H. Spanier, *Algebraic topology*, McGraw-Hill Book Company, New York, 1966.

College of Education
Ryukyu University
Nishihara, Okinawa, Japan

Polynomial Root Dragging

Bruce Anderson

1. INTRODUCTION. Rolle's Theorem and other results (such as those found in M. Marden **[1]** and anthologized in E. Barbeau **[2]**) furnish insight about the location of the zeros of the derivative of a polynomial (i.e. the critical points) relative to the location of the zeros of the polynomial. These results tend to be "static" in that they indicate where the critical points should be expected within certain bounds defined by the fixed location of the roots of $p(x)$ (e.g. within intervals bounded by the roots of the polynomial for real roots, or within a complex hull for the complex case). This paper will, in contrast, explore a simple "dynamic" result, showing how the roots of the derivative will be "affected" as we move (or drag) the roots of the polynomial, provided all the roots are real. The results are given in Theorem 2.1 and Corollary 2.2. We then show that this result does not generalize to complex roots in the obvious way.

The root dragging result of Corollary 2.2 is then employed to address the questions: Do the quartic polynomials produce all possible arrangements of critical points which satisfy Rolle's theorem? Or are there additional constraints on the possible arrangement of real critical points for quartics? Theorem 3.1 will furnish the perhaps surprising answer.

2. ROOT DRAGGING. Let $p(x)$ be a polynomial of degree n with all real distinct roots $x_1 < x_2 < \cdots < x_n$. Suppose we "drag to the right" some or all of these roots. I.e. we construct a new nth degree polynomial q with all real distinct roots $x'_1 < x'_2 < \cdots < x'_n$ such that $x'_i > x_i$ for all integers i between 1 and n. The derivatives of p and q, which of course are polynomials of degree $n-1$, must also have all real distinct roots from Rolle's theorem. Let $z_1 < z_2 < \cdots < z_{n-1}$ and $z'_1 < z'_2 < \cdots < z'_{n-1}$ be the roots of p' and q', respectively. (By Rolle's theorem, $x_k < z_k < x_{k+1}$ and $x'_k < z_k < x'_{k+1}$ for all integers k between 1 and $n-1$).

Theorem 2.1. (Root Dragging Theorem). *The roots of q' will each be to the right of the corresponding roots of p'; i.e. $z'_k > z_k$ for all integers k between 1 and $n - 1$.*

Proof: Our analysis will be in the spirit of the proof of the Gauss-Lucas Theorem found in Marden [1]. We suppose there is some k such that the corresponding roots, z_k and z'_k, are *not* in the order guaranteed by the theorem, i.e. $z'_k < z_k$. We show this leads to a contradiction. As shown in Marden [1], we know that the root z_k of p' must satisfy the equation:

$$\sum_{i=1}^{n} \frac{1}{z_k - x_i} = 0. \tag{1}$$

Likewise, the root z'_k of q' must satisfy:

$$\sum_{i=1}^{n} \frac{1}{z'_k - x'_i} = 0. \tag{2}$$

But since $x'_i > x_i$ and $z'_k < z_k$ (by assumption) we conclude:

$$z'_k - x'_i < z_k - x_i \tag{3}$$

Now, since z_k lies between x_k and x_{k+1} and z'_k lies between x'_k and x'_{k+1}, both sides of inequality (3) will be of the same sign. Thus

$$\frac{1}{z'_k - x'_i} > \frac{1}{z_k - x_i}. \tag{4}$$

Since this is true for all i, sums (1) and (2) cannot both equal zero. Q.E.D.

Corollary 2.2. *Let p and q be the same polynomials described in the theorem above. The roots of any derivative $q^{(j)}$ will each be to the right of the corresponding roots of $p^{(j)}$. I.e. if we shift roots of p to the right, the roots of all its derivatives will also shift to the right.*

Proof: Follows easily by induction on j. Q.E.D.

Remarks 2.3. (i) With a little care the requirement that the roots be distinct (i.e. no multiple roots) may be dropped. (ii) Essentially Corollary 2.2 says that the roots of the derivatives of a polynomial "follow" the roots of the polynomial (assuming all the roots are real). A more refined analysis which will not be presented here gives the following result: The roots of the derivatives will all move faster than the slowest moving root of the polynomial and slower than the fastest moving root of the polynomial.

3. APPLICATION OF THE ROOT DRAGGING THEOREM. Let $p(x)$ be a fourth degree polynomial whose (four) roots are all real and distinct. Call the inner two roots a_1 and a_2. Now by Rolle's theorem, $p'(x)$ must have exactly three real distinct roots. Call the middle root b. Iterating Rolle's, $p''(x)$ must have two real distinct roots (which we call c_1 and c_2), and $p^{(3)}$ must have one real root, d. By elementary analysis, d will be the average value of the four roots of $p(x)$.

Theorem 3.1 (Unconstructible fourth degree polynomial). *If $a_1 < c_1$ and $a_2 < c_2$ then $b < d$.*

Remarks 3.2. Figure 1 illustrates the arrangement of roots which Theorem 3.1 states is unconstructible. Here "0" represents the location along the real number line of a root of p, "1" represents a root of p', and so on).

```
0           0                 0                0
    1        \        1        \        1
              2      /          2
                    3
```

Figure 1. Theorem 3.1 states that this arrangement of roots is unconstructible, where "0" represents the location of a root of $p(x)$, "1" represents the location of a root of $p'(x)$ and so on.

Proof of Theorem 3.1: Begin shifting the right-most "0" to the right. Since the location of the "3" is the average of the "0's" and since the middle "1" must lie between the second and third "0's" by Rolle's Theorem, the "3" must eventually line up with the middle "1" as we continue shifting the right-most "0" to the right. Meanwhile, by Corollary 2.2, the 2's must shift to the right. Thus if the polynomial represented by Figure 1 is constructible, then so must Figure 2.

This means the polynomial must be symmetric around the middle "1", since we have a fourth degree polynomial with the first and third derivatives equal to zero there. But clearly the ordering depicted in Figure 2 is not symmetric. Q.E.D.

```
0           0                 0                0
    1        \        1        \        1
              2       |         2
                      3
```

Figure 2. By shifting the right most "0" to the right, we will eventually reach this arrangement of roots.

4. GENERALIZATIONS. One might ask whether there is an obvious complex generalization to Corollary 2.2. If we have a polynomial with complex roots, and we move all the roots in one direction, will the roots of the derivative all follow? The answer, as expected, is no, as illustrated by the following counterexample: Take the third degree polynomial p which has complex roots i, $-i$, and a real root of value 2. One can check that the roots of p' are $\frac{1}{3}$ and 1. But if we shift to the right the real root of p from 2 to say 3, the roots of the derivative become $1 - \sqrt{\frac{2}{3}}$ and $1 + \sqrt{\frac{2}{3}}$. Since

$$1 - \sqrt{\frac{2}{3}} < \frac{1}{3} < 1 < 1 + \sqrt{\frac{2}{3}}$$

the two roots of the derivative did not *both* shift to the right.

REFERENCES

1. M. Marden, *Geometry of Polynomials*, American Mathematical Society, Providence, 1966.
2. E. J. Barbeau, *Polynomials*, Springer-Verlag, New York, 1989.

Department of Mathematics
DePaul University
Chicago, IL 60614
anderson@math.cornell.edu

COMPUTER SCIENCE SAMPLER

Edited by: **Catherine C. McGeoch**

Parallel Addition

Catherine C. McGeoch

If you set nine women to digging a ditch they will complete it in one-ninth the time required by a single woman. But nine women working together cannot bear a child in one month. The moral: some tasks can be *parallelized* and some cannot.

Can addition be parallelized? If one person can add two n-digit integers in n seconds, can n people add them in one second? It appears that n-digit addition requires n seconds no matter how many people are working on it, since the high-order digits cannot be added until the high-order carry-in is known. But in fact there does exist a method for adding integers in about $2\log_2 n$ steps (using n people). The method is called *carry-lookahead addition* and is incorporated into the circuitry of nearly all modern computers. In this column we will look at carry-lookahead addition as well as an interesting parallel method for adding three integers.

We shall work with nonnegative n-digit integers expressed in binary (base two). Let X and Y be two such integers and let Z be their $n + 1$-digit sum. The digits of X are denoted $x_{n-1}x_{n-2}\dots x_1x_0$, and the digits of Y and Z are denoted similarly. Let $C = c_nc_{n-1}\dots c_1c_0$ represent the carry digits: that is, c_i is the *carry-in* added to x_i and y_i, and equivalently, the *carry-out* generated by adding x_{i-1}, y_{i-1} and c_{i-1}. We include c_0 for notational convenience, recognizing that $c_0 = 0$ always.

Figure 1-a contains a table defining one-digit binary addition with carry-ins and carry-outs. On the sixth line of the table, for example, we see that $1 + 0 + 1 = 10$

x	y	c_{in}	c_{out}	z
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

(a)

$$\begin{array}{lccccccc}
T & p & p & g & k & p & g & k \\
C & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
X & & 1 & 0 & 1 & 0 & 0 & 1 \\
Y & + & 0 & 1 & 1 & 0 & 1 & 1 \\
\hline
Z & 1 & 0 & 0 & 0 & 1 & 0 & 0
\end{array}$$

(b)

Figure 1

in base two. Figure 1-b gives an example 6-digit sum, showing C, X, Y, Z and a row labeled T (described below). The usual way to add is to apply the one-digit function to the digits of X, Y, and C in turn as i goes from 0 to $n-1$. The amount of time this takes (assuming constant time for each one-digit addition) is proportional to n. To achieve faster parallel addition we have to try something else.

Carry Lookahead Addition. Notice that we can sometimes calculate c_i without waiting to know the value of c_{i-1}. If x_{i-1} and y_{i-1} are both 0, then c_i must be 0, no matter what value c_{i-1} takes. Similarly, if x_{i-1} and y_{i-1} are both 1, then c_i must also be 1. The only problem arises when exactly one of x_{i-1} and y_{i-1} is 1, in which case c_i can't be determined until c_{i-1} is known.

We construct a *carry status* function f_i to reflect this situation. The carry status is expressed in terms of three functions k, g and p, each with domain $\{0, 1\}$. They are called the *kill* function, defined by $k(c) = 0$; the *generate* function $g(c) = 1$; and the *propogate* function $p(c) = c$. (You may recognize them by other names.) The carry status function is defined by

$$f_i(\cdot) = \begin{cases} k(\cdot) & \text{if } x_{i-1} = y_{i-1} = 0 \\ g(\cdot) & \text{if } x_{i-1} = y_{i-1} = 1 \\ p(\cdot) & \text{if } x_{i-1} \neq y_{i-1} \end{cases}$$

Row T in Figure 1-b shows the carry status functions for the example sum. It is easy to verify that $c_i = f_i(c_{i-1})$. Furthermore, we can apply function composition to obtain $c_i = f_i \circ f_{i-1}(c_{i-2})$. The handy table below shows the nine possible results of composing pairs of functions from $\{k, g, p\}$.

$\circ$	k	g	p
k	k	k	k
g	g	g	g
p	k	g	p

In general, $c_i = f_i \circ f_{i-1} \circ \cdots \circ f_j(c_{j-1})$ for $i > j > 0$. In particular, we have $c_i = f_i \circ \cdots \circ f_1(0)$, since by definition $c_0 = 0$. We will adopt the shorthand notation $[i, j]$ to refer to a sequence of compositions $f_i \circ \cdots \circ f_j$. In this notation $f_i = [i, i]$ and $c_i = [i, 1](0)$ for i between 1 and n. We stretch the notation slightly to let $c_0 = [0, 1](0) = 0$.

Carry-lookahead addition uses a clever two-pass scheme to find all the carries c_i quickly. In the first pass several compositions $[i, j]$ are calculated. In the second pass, functions of the form $[i, j](c_{j-1})$ are evaluated, one for each i between 1 and n. Once all the carry values $c_i = [i, j](c_{j-1})$ are known, the individual sums $x_i + y_i + c_i$ can be found simultaneously to produce the digits of Z.

Figure 2 shows a *combinational circuit* for performing carry-lookahead on 8-bit integers. The circuit comprises several *nodes* connected together by directed *wires*. The wires carry *values*: a node sends a value on its output wire according to some fixed function of values on its input wires. We require that each node have a fixed number of input wires and output wires, and that each node execute its function(s) in a fixed amount of time.

The circuit contains 7 *oval* nodes arranged in a binary tree, 1 *circle* node attached to the root of the tree, and 8 *square* nodes at the leaves of the tree. These different types of nodes perform different functions. In general, $n-1$ ovals, 1

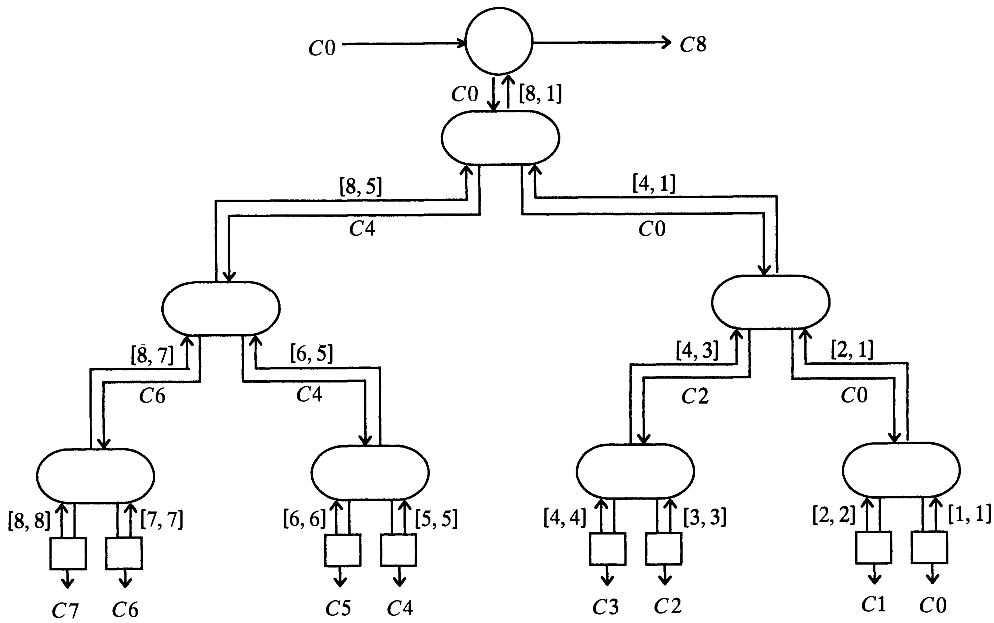


Figure 2

circle, n squares, and n more *adder nodes* (not shown here) are required for n-bit addition when n is a power of 2.

We can now add X and Y as follows.

Step 1. The n square nodes calculate $[i, i] = f_i(\cdot)$, for i in $1 \dots n$, each using inputs x_{i-1} and y_{i-1} (not shown in Figure 2). Each square node sends the appropriate value **k**, **g**, or **p** along its output wire going up. This step requires $\Theta(1)$ time[1] since the square nodes can operate simultaneously.

Step 2. Each oval node performs the composition $[i, j] = [i, k] \circ [k - 1, j]$ *going up*. That is, the function values for $[i, k]$ and $[k - 1, j]$ (each is either **k**, **g**, or **p**) are obtained from neighbor nodes below and the result $[i, j]$ is passed to the neighbor above. The circle node at top eventually receives $[n, 1]$. The arrows pointing up in Figure 2 are labelled to show the flow of values in this step. Overall, the time required for values to move from the square nodes (where the initial $[i, i]$ values are located) to the circle node (the last one to receive a value) is $\Theta(\log n)$.

Step 3. The circle node evaluates $[n, 1](0)$, equivalent to c_n. It also passes $c_0 = 0$ down to the root oval. Each oval node evaluates

$$c_{k-1} = [k - 1, j](c_{j-1})$$

going down. To accomplish this the node retains $[k - 1, j]$ from Step 2 and receives c_{j-1} from the neighbor above. The result c_{k-1} is passed down to the left neighbor, and c_{j-1} is passed down to the right. The arrows pointing down in Figure 2 are labeled to show the flow of values in this step. The total time required for values to propogate from the circle node down to the square nodes is $\Theta(\log n)$.

[1]The notation $\Theta(f(n))$ means "proportional to $f(n)$" in the following sense: $g(n) = \Theta(f(n))$ means that there exist positive constants a and b and n_0 such that for all $n > n_0$ we have $af(n) \le g(n) \le bf(n)$. For example any constant function is $\Theta(1)$ and any function of the form $d \log_2 n + e$ (for constants d and e) is $\Theta(\log n)$.

Step 4. The circle node has computed c_n, and the square nodes now hold the carry values c_i for i between 0 and $n-1$. These values can be passed to an array of adder nodes that simultaneously perform the 3-bit additions $x_i + y_i + c_i$ (discarding the carry-outs) to obtain the digits z_i of Z. This final step takes $\Theta(1)$ time.

The total amount of time required for the lookahead circuit and the adder array to form the sum of X and Y is $T(n) = L(n) + A(n)$, where $L(n) = \Theta(\log n)$ (to find the carry digits by lookahead) and $A(n) = \Theta(1)$ (to add the one-bit triples). Therefore $T(n) = \Theta(\log n)$. Note that although the circuit contains $3n$ nodes, carry-lookahead addition could be performed by n people acting as nodes, since people can move around and change functions.

Carry Save Addition. Now, how long does it take to add three n-digit integers W, X, and Y? We could certainly add Y to the $n+1$-digit sum of W and X; this would require $2T(n+1)$ time if we use a lookahead-adder circuit of size $n+1$ twice. A better idea is to apply *carry save* addition, which only requires $\Theta(1) + T(n+1)$ time.

Given n-digit W, X, and Y, a carry save adder constructs two intermediate integers, an $n+1$ digit U and an n-digit V, such that $U + V = W + X + Y$. Then U and V are summed with a carry-lookahead adder circuit of size $n+1$.

Here's how it works. Referring again to Table 1-a, let the binary integer uv denote the 2-digit sum of three 1-digit binary integers; that is, $w + x + y = uv$. Then it must be the case that $w + x + y = 2u + v$.

For each i in $0 \ldots n-1$, apply the function in Table 1-a to the digits w_i, x_i, and y_i of W, X, and Y. Set $v_i = z$ and $u'_i = c_{out}$ as labelled in the table, and let v_i and u'_i denote the digits of V and U', respectively. Let U be defined by $u_0 = 0$ and $u_i = u'_{i-1}$ for i in $1 \ldots n$. Then V and $U = 2U'$ are the desired intermediate integers, since

$$
\begin{aligned}
W + X + Y &= \sum_{i=0}^{n-1} (w_i + x_i + y_i)2^i \\
&= \sum_{i=0}^{n-1} (2u'_i + v_i)2^i \\
&= \sum_{i=0}^{n-1} u'_i 2^{i+1} + v_i 2^i \\
&= \sum_{i=0}^{n-1} u_{i+1} 2^{i+1} + \sum_{i=0}^{n-1} v_i 2^i \\
&= U + V.
\end{aligned}
$$

The digits v_i and u_i can be calculated simultaneously by n adder nodes in $\Theta(1)$ time. After that, U and V can be added by a carry-lookahead circuit of size $n+1$ in $T(n+1)$ time.

Further Reading. Carry-lookahead addition and carry save addition have been around since the middle 1960's. We have since figured out how to parallelize several other arithmetic operations. For example, carry-save addition can be generalized so that a circuit containing $\Theta(nm)$ modes can be used to add m n-digit numbers in $\Theta(\log_2 m + \log_2 n)$ time steps. This implies that two n-digit numbers can be *multiplied* in $\Theta(\log_2 n)$ time steps. We also know that under the standard

formal model of parallel computation it is *not* possible to add two n-digit numbers in $\Theta(1)$ time.

Two recent texts by Cormen et al. [1] and by Leighton [2] give excellent discussions of parallel arithmetic. The search for efficient parallel algorithms for general computational problems is a vigorous research area of theoretical computer science; Leighton's text, in particular, gives a comprehensive view of the state of the art.

ACKNOWLEDGMENT. This seems a good time to thank Dan Velleman for outstanding service as a "typical mathematical audience". Dan's insightful suggestions and comments on draft columns are most gratefully acknowledged.

REFERENCES

1. T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introduction to Algorithms*, MIT Press, 1990.
2. F. T. Leighton, *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes*, Morgan Kaufmann, 1992.

Department of Mathematics and Computer Science
P.O. Box 2239
Amherst College
Amherst, MA 01002
ccm@cs.amherst.edu

Word has reached this country that the Editor of the *Zentralblatt für Mathematik und ihre Grenzgebiete*, Professor Otto Neugebauer, now of Copenhagen, has resigned. The resignation from this mathematical abstracts journal was occasioned by the action of the publisher, Julius Springer of Berlin, in dropping Professor Levi-Civita of Italy from the board without the knowledge of the Editor, as well as by the demand that the Editor give assurance that no emigrants would be allowed to referee articles by German authors. In consequence of this interference with editorial policies, the American associate editors, Professors Tamarkin and Veblen, have tendered their resignations as have also a number of associate editors and collaborators in other countries.

—*American Mathematical Monthly*
46 (1939), p. 57

PROBLEMS AND SOLUTIONS

Edited by:
Richard T. Bumby, Fred Kochman and Douglas B. West

Proposed problems should be sent to the MONTHLY PROBLEMS address given on the inside front cover. Please include solutions, relevant references, etc. Three copies are requested.

Solutions of published problems should arrive before April 30, 1994 at the MONTHLY PROBLEMS address given on the inside front cover. Solutions should be typed with double spacing, including the problem number and the solver's name and mailing address. Two copies suffice. A self-addressed postcard or label should be included if an acknowledgment is desired.

*An asterisk (*) after the number of a problem, or part of a problem, indicates that no solution is currently available. Partial solutions will be useful in such cases. Otherwise, the published solution is likely to be based on a solution which is complete and correct. Of course, an elegant partial solution or a method leading to a more general result is always useful and welcome. In addition, references to other appearances of MONTHLY problems or to solutions of these problems in the literature are also solicited.*

PROBLEMS

10338. *Proposed by Charles Vanden Eynden, Illinois State University, Normal, IL.*

Given an integer $n > 1$, determine the set of integers which can be written as a sum of two integers relatively prime to n.

10339. *Proposed by Moshe Rosenfeld, Pacific Lutheran University, Tacoma, WA.*

Let A and B be complex matrices with $AB^2 - B^2A = B$. Prove that B is nilpotent.

10340. *Proposed by Richard Bagby, New Mexico State University, Las Cruces, NM.*

For a normed linear space $\mathbf{X}$ and $x \in \mathbf{X}$, define

$$P(x) = \{y \in \mathbf{X}: \|x + y\|^2 = \|x\|^2 + \|y\|^2\}.$$

If the norm in $\mathbf{X}$ comes from an inner product, then each $P(x)$ is invariant under multiplication by real numbers. Is the converse true?

10341. *Proposed by George Cain and Zhiging Lu (student), Georgia Institute of Technology, Atlanta, GA.*

Let $\mathbf{D} = \{(x, y)\colon\ x^2 + y^2 \leqslant 1\}$ be the unit disk in the plane, and let $\{A_1, A_2, \ldots, A_n\}$ be a pairwise disjoint collection of finite subsets of the set $\mathbf{C} = \{(x, y)\colon\ x^2 + y^2 = 1\}$. Prove that there is a pairwise disjoint collection $\{K_1, K_2, \ldots, K_n\}$ of connected subsets of $\mathbf{D}$ such that $A_i \subset K_i$ for each $i = 1, 2, \ldots, n$.

10342. *Proposed by Shmuel Rosset, Tel Aviv University, Ramat Aviv, Israel.*

Let F be a free group, and R a normal subgroup of F. Consider the subgroups $[R, nF]$ defined by

$$[R, nF] = \begin{cases} R & \text{if } n = 0, \\ [[R, (n-1)F], F] & \text{if } n > 0. \end{cases}$$

Prove that the set of elements of finite order in $R/[R, nF]$ is an abelian group.

10343. *Proposed by David M. Bloom, Brooklyn College, CUNY, Brooklyn, NY.*

Let us call a subset of $\mathbb{Z}$ *semi-unfriendly* (abbreviated *S-U*) if it contains no *three* consecutive integers. Let E_n denote the n element set $\{1, 2, \ldots, n\}$, and let

$$A(n, k) = \#\{S \subset E_n\colon \#S = k,\ S \text{ is } S\text{-}U\}$$

$$B(n, k) = \#\{S \subset E_n\colon \#S = k,\ S \text{ is } S\text{-}U \text{ and } E_n - S \text{ is } S\text{-}U\}.$$

Prove that

$$B(3n - 1, n) = A(n + 3, 3)$$

for all $n \geqslant 1$.

10344*. *Proposed by E. Ehrhart, Université de Strasbourg, Strasbourg, France.*

Let $\mathscr{S}$ be a regular tetrahedron, and let $P \in \mathscr{S}$. Define $\mathbf{D}_V(P)$ to be the sum of the distances from P to the vertices of $\mathscr{S}$, and $\mathbf{D}_E(P)$ to be the sum of the distances from P to the edges of $\mathscr{S}$. Find the maximum and minimum values of $\mathbf{D}_E(P)/\mathbf{D}_V(P)$.

10345. *Proposed by George Baloglou, SUNY College at Oswego, Oswego, NY, and Fred Galvin, University of Kansas, Lawrence, KS.*

Given a subset $\mathbf{X} \subset \mathbb{R}$ one obtains a subset $\mathbb{R}^2 \setminus \mathbf{X}^2$ of the plane by removing those points both of whose coordinates are in $\mathbf{X}$. If $\mathbf{X} \neq \mathbb{R}$, such a set always contains horizontal and vertical lines.

(a) Find such a set $\mathbf{X}$, of Lebesgue measure zero, for which $\mathbb{R}^2 \setminus \mathbf{X}^2$ contains no circles.

(b)* Is there such a set $\mathbf{X}$, of Lebesgue measure zero, for which every connected subset of $\mathbb{R}^2 \setminus \mathbf{X}^2$ consisting of more than one point contains a horizontal or vertical line segment?

NOTES

Notes: (10339) An element, B, of a ring is called *nilpotent* if there is a positive integer k for which $B^k = 0$. For the ring of n by n matrices over the complex numbers, for fixed n, it would be of interest to seek a complete characterization of the solutions of the equation of this problem. **(10342)** Here, the symbol $[A, B]$ stands for the group generated by the commutators $aba^{-1}b^{-1}$ with $a \in A$ and $b \in B$. If A is a normal subgroup of B, so is $[A, B]$. A reference for free groups is Magnus, Karrass, & Solitar, *Combinatorial Group Theory*. **(10344)** This problem is listed as "unsolved" and no bounds are stated although partial results including conjectured extreme values are available, because these results are supported only by numerical evidence.

SOLUTIONS

Six Barycenters in Search of a Conic

E3469 [1991, 955]. *Proposed by Hüseyin Demir, Middle East Technical University, Ankara, Turkey.*

Suppose P is a point in the interior of triangle ABC and suppose AP, BP, CP meet the lines BC, CA, AB respectively at the points D, E, F. Prove that the centroids of the six triangles $PBD, PDC, PCE, PEA, PAF, PFB$ lie on a conic if and only if P lies on at least one of the three medians of the triangle.

Restatement of problem and fixing of notation. Applying the homothety with center P and ratio $3:2$ we see that the centroids of triangles are on a conic if and only if the midpoints of AF, FB, BD, DC, CE and EA are on one conic. Let x, y, z, u, v, w denote half the lengths of AF, FB, BD, DC, CE, EA, respectively. Let the midpoints of AF, FB, BD, DC, CE, EA be denoted by $1, 2, 4, 5, 6$ respectively.

Solution I by Victor Prasolov, Independent University of Moscow, Moscow, Russia.

By Carnot's Theorem (see Howard W. Eves, *A survey of geometry* (Revised Edition), Allyn and Bacon, 1972, pages 256 and 262) the six centroids lie on a conic if and only if

$$x(2x+y)z(2z+u)v(2v+w) = w(2w+v)u(2u+z)y(2y+x). \quad (1)$$

By Ceva's Theorem, $xzv = wuy$, so (1) simplifies to $xzw + zvy + vxu - (wux + uyv + ywz) = 0$, or $(x-y)(z-u)(w-v) = 0$. This condition corresponds to P lying on a median.

Solution II by Albert Nijenhuis, Seattle, WA. By Pascal's Theorem, the points 1, 2, 3, 4, 5, and 6 lie on a conic if and only if the three points $Q = AB \cap 45$, $R = BC \cap 61$ and $S = CA \cap 23$ are collinear. (There is no real difficulty if any of these points are at infinity. The ratio AQ/QB, for example, is replaced by -1 if $AB \| 45$.)

By Menelaus' Theorem, we have

$$\frac{AQ}{QB} \cdot \frac{2z+u}{u} \cdot \frac{v}{2w+v} = -1, \qquad \frac{BR}{RC} \cdot \frac{2v+w}{w} \cdot \frac{x}{2y+x} = -1,$$
$$\frac{CS}{SA} \cdot \frac{2x+y}{y} \cdot \frac{z}{2u+z} = -1.$$

Multiplying these together and using Ceva's theorem, as in Solution I, we see that $AQ/QB \cdot BR/RC \cdot CS/SA = -1$ if and only if $(x-y)(z-u)(w-v) = 0$. Thus Q, R, S are collinear and hence the points $1, 2, 3, 4, 5, 6$ lie on a conic if and only if P is on a median.

Comments by Neela Lakshmanan, University of Scranton, Scranton, PA. The restriction that P is interior to the triangle may be relaxed: we need only that P does not lie on any side of the triangle.

We can prove that the result is true not only for the midpoints but also for the points that divide each of those six segments in a *constant ratio*: If $1, 2, 3, 4, 5, 6$ are points on the sides of the triangle defined by $A1:1F = F2:2B = B3:3D = D4:4C = C5:5E = E6:6A$, then the six points lie on a conic if and only if P is on a median. Also, if P is an interior point, the hexagon $1, 2, 3, 4, 5, 6$ is convex and attains its maximum area when P is the centroid of $\triangle ABC$.

Editorial comment. Many of the solvers supplemented the use of Carnot's Theorem or Pascal's Theorem with homogeneous coordinates and analytic methods. Some others worked directly with conditions on the six coefficients of a general conic.

Solved also by F. Bellot and M. A. Lopéz (Spain), R. J. Chapman (U.K.), J. Fukuta (Japan), H. Kappus (Switzerland), O. P. Lossers (The Netherlands), I. A. Sakmar (Turkey), Anchorage Math Solutions Group, and the proposer. One incorrect solution was received.

Periodicity of a Sign Function

E 3471 [1991, 955]. *Proposed by William Calbeck, Florida International University, Miami, FL, and Bruce Reznick, University of Illinois, Urbana, IL.*

Let P_k be the set of all integer-valued polynomials of degree at most k, i.e., the set of all polynomials p of degree at most k such that $p(n) \in \mathbb{Z}$ for $n \in \mathbb{Z}$. (It is known that $p \in P_k$ if and only if

$$p(x) = a_0 + a_1\binom{x}{1} + a_2\binom{x}{2} + \cdots + a_k\binom{x}{k},$$

where $a_0, a_1, a_2, \ldots, a_k$ are integers.) Let $r(k)$ be the smallest power of 2 strictly greater than k.

(a) If $p \in P_k$, show that the sequence $\{(-1)^{p(n)}\}_{n=1}^{\infty}$ is periodic with period $r(k)$.

(b) Show that any given sequence of plus and minus ones with period 2^n occurs for some p in P_{2^n-1}.

Solution to part (a) by Robin J. Chapman, University of Exeter, UK. It suffices to show that if $j < 2^s$ and $m \in \mathbb{Z}$, then $\binom{m}{j} \equiv \binom{m+2^s}{j} \bmod 2$. These are the coefficients of x^j in the power series $(1+x)^m$ and $(1+x)^{m+2^s}$, respectively. The congruence $(1+x)^{2^s} \equiv 1 + x^{2^s} \bmod 2$ follows easily by induction on s. Hence $(1+x)^{m+2^s} \equiv (1+x)^m(1+x^{2^s}) \bmod 2$. Since j is less than 2^s, it is immediate that the coefficients of x^j in $(1+x)^m$ and $(1+x)^{m+2^s}$ have the same parity.

Solution to part (b) by Albert Nijenhuis, Seattle, WA. Let $a_0, \ldots, a_{2^n-1}$ be arbitrary integers, and let $b_0, \ldots, b_{2^n-1}$ be the solution to the equations

$$\sum_{i=0}^{2^n-1} b_i \binom{j}{i} = a_j \quad \text{for } 0 \leqslant j \leqslant 2^n - 1.$$

The matrix of this system is lower triangular, with 1's on the main diagonal, so $\{b_i\}$ are integers. The polynomial $\sum_{i=0}^{2^n-1} b_i \binom{x}{i}$ realizes the sequence $\{(-1)^{a_j}\}_{j=0}^{2^n-1}$ and its extension with period 2^n.

Editorial comment. Solvers used various methods; several cited theorems of Kummer and Lucas. William F. Trench recognized the problem as E 1365 [1959, 312; 1959, 919], proposed by M. E. Hausner and solved by N. J. Fine, and noted that a generalization to modulus m appears in William F. Trench, "On periodicities of certain sequences of residues," this MONTHLY 67 (1960), 652–656. Problem E 1365 had only two solvers in 1959.

Solved also by D. Callan, M. Dindos (Slovakia), F. J. Flanigan, R. High, K. S. Kedlaya (student), O. P. Lossers (The Netherlands), R. Martin (student), M. D. Meyerson, A. Pedersen (Denmark), W. F. Trench, Anchorage Math Solutions Group, National Security Agency Problems Group, and the proposer.

Arbitrarily Periodic Sequences

10184 [1992, 60]. *Proposed by Gerry Myerson, Macquarie University, New South Wales, Australia.*

Is there a sequence of natural numbers having the following two properties:
(i) The sequence is periodic modulo m for every positive integer m,
(ii) each natural number appears in the sequence infinitely often?

Solution I by Kiran S. Kedlaya (student), Harvard University, Cambridge, MA. Yes. The following algorithm constructs such a sequence. Let S_1 be the sequence whose one term is 1. For $n \geqslant 1$, recursively define S_{n+1} by appending to the end of S_n the sequences $S_n + 0 \cdot n!, S_n + 1 \cdot n!, \ldots, S_n + n \cdot n!$, where $T + k$ denotes the finite sequence obtained by adding k to each term of T. Let S be the sequence generated by this procedure as $n \to \infty$.

To prove that S satisfies (i), note that for all $n > m$, we obtain S_n by appending blocks that are congruent to S_m modulo m. Hence S is periodic modulo m with period dividing the length of S_m, which is seen by induction to be $(m+1)!/2$.

To verify that S satisfies (ii), first note by induction that S_n contains $\{1, \ldots, n!\}$. Then observe that every number in S_n occurs at least twice as often in S_{n+1}. Thus every natural number appears in S infinitely often.

Solution II by Richard Stong, University of California, Los Angeles, CA. For each $n \geqslant 0$, there are unique integers $c_1, \ldots, c_k$ with $0 \leqslant c_j \leqslant j$ such that $n = \sum_{j=1}^{k} c_j j!$. Let $g(x) = \max\{0, x - 1\}$ and define $a_n = \sum_{j=1}^{k-1} g(c_{j+1}) j!$.

Condition (i) holds for $\{a_n\}$ because $a_{n+(m+1)!} \equiv a_n \bmod m!$. To verify condition (ii), note that if $n = \sum_{j=1}^{k} c_j j!$, then $a_r = n$ for any r of the form $r = \sum_{j=1}^{s} b_j j!$ with $s > k$ and

$$b_j = \begin{cases} c_{j-1} + 1 & \text{if } 2 \leqslant j \leqslant k+1 \\ 0 \text{ or } 1 & \text{otherwise} \end{cases}.$$

Editorial comment. Richard Stong's solution was the only submission giving an explicit formula for the nth term of the sequence; most solvers gave recursive procedures. Solvers disagreed on whether the natural numbers include 0. For this problem the question is moot, as the periodicity is unaffected by adjusting each term by 1. The proposer observed that "natural numbers" can be replaced by "integers" by alternating the terms of S with the terms of $1 - S$.

Solved also by M. Dasef & S. Kautz, P. Flor (Austria), J. Gonzalez-Meneses (student, Spain), J. W. Grossman, T. Hesterberg, R. High, N. Kang (student, Korea), U. Klein (student, Germany), O. P. Lossers (The Netherlands), M. D. Meyerson, A. Nijenhuis, I. Praton, A. Riese, R. M. Robinson, T. W. Starbird, D. M. Wells, GCHQ Problem Solving Group (U.K.), Theory First, University of South Alabama Problem Group, and the proposer.

A Golden Oldie

10193 [1992, 161]. *Proposed by Solomon Golomb, University of Southern California, Los Angeles, CA.*

Determine all pairs of integers n, k such that

$$\binom{n}{k} = \binom{n+1}{k-1}, \qquad n > k > 1.$$

Solution by Christos Athanasiadis (student), Massachusetts Institute of Technology, Cambridge, MA. All such pairs are given by $n = F_{2m+1}F_{2m} - 1$, $k = F_{2m}F_{2m-1}$ for $m = 2, 3, \ldots$. Here $\langle F_m \rangle_{m=1}^{\infty}$ is the Fibonacci sequence defined by $F_1 = F_2 = 1$ and $F_{m+2} = F_{m+1} + F_m$.

To see this, first note that the given condition can be written as

$$(n+1)k = (n-k+1)(n-k+2)$$

or as

$$(p+k)k = p(p+1), \tag{1}$$

where $p = n - k + 1$. Let $p = rt$, $k = st$ with $(r, s) = 1$. Then (1) becomes $(r+s)st^2 = rt(rt+1)$. It follows that t divides r, so that $r = tr_1$ and $(r+s)s = r_1(rt+1)$. Since r_1 is relatively prime to s and hence also to $r + s$, it must be that $r_1 = 1$. Hence $p = t^2$, $k = st$, and $t^2 + 1 = s(t+s)$. We need the following lemma.

Lemma. *The integer solutions to*

$$t^2 + 1 = s(t+s), \quad s \geq 1, t \geq 1 \tag{2}$$

are given by $s = F_{2m-1}$, $t = F_{2m}$ for $m = 1, 2, \ldots$.

Proof: The classical formula $F_{2m+1}F_{2m-1} - F_{2m}^2 = 1$ (easily proved by induction) shows that $s = F_{2m-1}$, $t = F_{2m}$ is a solution of (2) for $m = 1, 2, \dots$. (In particular $(1,1)$ is a solution.) We now use an argument by descent to show that there are no other solutions of (2). Suppose that s and t are positive integers satisfying (2) and that $(s,t) \neq (1,1)$. Put

$$\begin{pmatrix} v \\ u \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} t \\ s \end{pmatrix}, \quad \text{that is} \quad \begin{pmatrix} t \\ s \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} v \\ u \end{pmatrix}. \tag{3}$$

Since $t^2 + 1 = st + s^2 > 1 + s^2$, we have $s < t$. Since $st + s^2 > t^2$, we have $(s/t) + (s/t)^2 > 1$ and hence $s/t > (\sqrt{5} - 1)/2 > \frac{1}{2}$. Thus $t/2 < s < t$, which implies that $u = 2s - t$ and $v = t - s$ are positive integers. It is easy to verify that $v^2 + 1 - u(v + u) = t^2 + 1 - s(t + s)$, so that (u, v) is a solution of (2) with $0 < u < s$, $0 < v < t$.

It follows by repetition of this argument that

$$\begin{pmatrix} t \\ s \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{m-1}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

for some positive integer m greater than 1. A simple induction argument shows that

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{m-1} = \begin{pmatrix} F_{2m-1} & F_{2m-2} \\ F_{2m-2} & F_{2m-3} \end{pmatrix} \quad (m = 2, 3, \dots).$$

Hence, if (s, t) is any solution of (2) other than $(1, 1)$, we have

$$\begin{pmatrix} t \\ s \end{pmatrix} = \begin{pmatrix} F_{2m-1} & F_{2m-2} \\ F_{2m-2} & F_{2m-3} \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} F_{2m} \\ F_{2m-1} \end{pmatrix}$$

for some positive integer m greater than 1. Thus the lemma is proved.

In view of the lemma we have $k = st = F_{2m}F_{2m-1}$ and

$$n = p + k - 1 = t^2 + st - 1 = F_{2m}^2 + F_{2m}F_{2m-1} - 1 = F_{2m+1}F_{2m} - 1$$

for some integer m greater than 1, as claimed. The first five solutions (n, k) are (14, 6), (103, 40), (713, 273), (4894, 1870), and (33551, 12816).

Editorial comment. David M. Bloom and Savely Khosid each pointed out that the same problem appeared in the MONTHLY over sixty years ago as Problem 3459 [1930, 508; 1931, 551]. The above solution is more concise and direct than the solution published in 1931 (which used the theory of simple continued fractions). Problem 3459 is also the 65th problem in the collection of MONTHLY problems published as [**1**].

The problem is also treated in [**3**], [**4**], [**5**], and [**6**] (particularly pp. 32–34). These previous occurrences were called to our attention by B. M. M. de Weger, by Jean-Marie Pages and Dave Trautman, by Robert B. McNeill, and by Mark Sand respectively.

The diophantine equation $t^2 + 1 = s(t + s)$ of the above lemma may be written as $(2s + t)^2 - 5t^2 = 4$, an instance of the so-called Pell equation. (See, for example, Chapter 7 of Part One of [**2**].) Most solvers used the theory of the Pell equation or the theory of simple continued fractions. The selected solution bypasses the general theory, but uses knowledge of the small solutions of equation (2) to construct the change of variables in (3).

About one-third of the solvers obtained the result in the form $n = F_{2m}F_{2m+1} - 1$, $k = F_{2m}F_{2m-1}$, $m > 1$ given in the above solution. Several solvers included lists of pairs (n, k) produced by this formula. Some solvers, as well as reference [4], also gave the 29 digits of $\binom{103}{40}$. No one attempted to display the next value.

REFERENCES

1. The Otto Dunkel Memorial Problem Book, edited by Howard Eves and E. P. Starke, this MONTHLY, 64 (1957), no. 7, Part 2.
2. Edmund Landau, *Elementary Number Theory*, Chelsea Pub. Co., 1955.
3. D. A. Lind, "The quadratic field $Q(\sqrt{5})$ and a certain diophantine equation," *Fibonacci Quart.* 6, (1968), 86–93.
4. David Singmaster, "Repeated binomial coefficients and Fibonacci numbers," *Fibonacci Quart.* 13 (1975), 295–298.
5. Craig A. Tovey, "Multiple occurrences of binomial coefficients," *Fibonacci Quart.* 23 (1985), 356–358.
6. S. Vajda, *Fibonacci and Lucas Numbers, and the Golden Section*, Ellis Horwood Limited, 1989.

Solved by 88 readers and the proposer. Six incorrect solutions were also received.

Similar Orthic Triangles

10202 [1992, 265]. *Proposed by Juan Bosco Romero Márquez, Universidad de Valladolid, Valladolid, Spain.*

Let A', B', C' be the feet of the altitudes of $\triangle ABC$ and let X, Y, Z be the centers of the circumscribing rectangles of $\triangle ABC$ with edges BC, CA, AB respectively. Prove that $\triangle XYZ$ is a dilation of $\triangle A'B'C'$.

Solution I by Robin J. Chapman, University of Exeter, Exeter, U. K. There is an ambiguity as to what is meant by "circumscribing rectangle." The circumscribing rectangle of $\triangle ABC$ with edge BC may be defined as either:

(i) the rectangle $BCPQ$ where A lies on the line PQ (possibly extended); or

(ii) the smallest rectangle containing $\triangle ABC$, one of whose sides lies on the line BC.

These two definitions coincide provided neither $\angle ABC$ nor $\angle ACB$ is obtuse. The result is always true under interpretation (i), but false under interpretation (ii) whenever $\triangle ABC$ has an obtuse angle. In particular, if $\angle ABC$ is obtuse, then both X and Z coincide with the midpoint of AC, but $\triangle A'B'C'$ is not degenerate.

We adopt definition (i) and use vector methods. Choose the origin O to be the centroid of $\triangle ABC$. Let $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{a}', \mathbf{b}', \mathbf{c}', \mathbf{x}, \mathbf{y}, \mathbf{z}$ be the position vectors of $A, B, C, S, A', B', C', X, Y, Z$ respectively. The circumscribing rectangle of $\triangle ABC$ with edge BC has vertices B, C and the points with position vectors $\mathbf{b} + (\mathbf{a} - \mathbf{a}')$ and $\mathbf{c} + (\mathbf{a} - \mathbf{a}')$. Hence $\mathbf{x} = (\mathbf{a} + \mathbf{b} + \mathbf{c} - \mathbf{a}')/2 = -\mathbf{a}'/2$ as O is the centroid of $\triangle ABC$. Similarly $\mathbf{y} = -\mathbf{b}'/2$ and $\mathbf{z} = -\mathbf{c}'/2$. Hence $\triangle XYZ$ is obtained from $\triangle A'B'C'$ by a dilation of factor $-1/2$ centered at the centroid O of $\triangle ABC$.

Solution II by Shailesh Shirali, Rishi Valley School, Chittoor District, Andhra Pradesh, India. Let $\triangle DEF$ be the medial triangle of $\triangle ABC$ with vertex D opposite vertex A. Then it is easy to see that $\triangle XYZ$ is just the orthic triangle of $\triangle DEF$ with vertex X opposite vertex D. Now, a dilation about the centroid G of $\triangle ABC$ with scale factor $-1/2$ sends $\triangle ABC$ to $\triangle DEF$ and therefore sends the orthic triangle of $\triangle ABC$, namely $\triangle A'B'C'$, to that of $\triangle DEF$, namely $\triangle XYZ$.

Editorial comment. Solution II, like other solutions employing constructions of classical geometry, was accompanied by a drawing. Jordi Dou submitted such a diagram entitled "Proof without words." His diagram also highlights the fact, also observed by other solvers, that the dilation sending $\triangle XYZ$ to $\triangle A'B'C'$ also sends the circumcenter of $\triangle ABC$ (which is the orthocenter of the medial triangle) to its orthocenter, thereby exhibiting the fact that the centroid divides the segment joining the circumcenter and the orthocenter in the ratio of $1:2$ (the property of the Euler line).

Jiro Fukuta proved the following more general result. Let A', B', C' be any points on the sides BC, CA, AB, respectively. Let X be the center of the circumscribing parallelogram with one edge BC and the other pair of edges parallel to AA', and similarly for Y and Z. Then $\triangle XYZ$ is a dilation of $\triangle A'B'C'$, centered at the centroid of $\triangle ABC$, in the ratio of $-1/2$. This can be proved in the same way as the original problem, using either synthetic or vector methods. Since the lines AA', BB', and CC' are not required to be concurrent, this is more general than the affine version of the stated problem.

This generalization can be easily carried over to higher dimensions in the following manner. Let $A_0A_1 \dots A_n$ be a simplex in Euclidean n-space. For each $i = 0, 1, \dots n$, let A'_i be any point in the facet opposite A_i, and let X_i be such that the vector $X_i - G_i$ is equal to the vector $(A_i - A'_i)/n$, where G_i is the centroid of the facet. Then $X_0X_1 \dots X_n$ is a dilation of $A'_0A'_1 \dots A'_n$, centered at the centroid of the given simplex, in the ratio $-1/n$.

Solved also by E. Alkan (student, Turkey), P. J. Anderson (Canada), J. Anglesio (France), F. Bellot and M. A. Lopéz (Spain), P.-C. Chuang, A. Coffman, I. Dimitric, J. Dou (Spain), J. Fukuta (Japan), H. W. Guggenheimer, J. G. Heuver (Canada), H. Kappus (Switzerland), I. Kastanas, K. S. Kedlaya (student), N. Komanda, O. P. Lossers (The Netherlands), M. Lucian, H. M. Marston, R. Merrill, K. Perera (student), W. Reyes (Chile), B. Shawyer (Canada), A. Subramanian (student, India), T. C. Tran, M. Vowe (Switzerland), R. L. Young, and the University of Wyoming Problem Circle. The original proposal presented only a special case of the published problem.

Matrices with Agreeable Adjoints

10205 [1992, 266]. *Proposed by Richard Sinkhorn, University of Houston, Houston, TX.*

In elementary linear algebra, two different definitions of the word "adjoint" are used. The adjoint of a square matrix A with complex entries is either:

(I) the matrix whose (i, j)-entry is the cofactor of a_{ji} in A; or,

(II) the complex conjugate of the transpose of A.

Under what conditions on the matrix A will these two definitions yield the same matrix?

Solution by Peter Nylen, Tin-Yau Tam, and Frank Uhlig, Auburn University, Auburn, AL. There are three possibilities: (i) A is a zero matrix; (ii) A is unitary with $\det A = 1$; or (iii) A is a 2 by 2 matrix of the form

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}.$$

We use adj A for the first "adjoint" and A^* for the second. The above matrices all satisfy $A^* = \operatorname{adj} A$. Notice that $(\operatorname{adj} A)A = A(\operatorname{adj} A) = (\det A)I$. If $A^* =$

adj A, then

$$A^*A = AA^* = (\det A)I. \tag{1}$$

Since AA^* is positive semi-definite, $\det A \geqslant 0$. By taking the trace of both sides of (1), it follows that A is either nonsingular or zero. If A is nonsingular, take the determinant of both sides of (1). Then $|\det A|^2 = (\det A)^n$. Hence, if $n \neq 2$, $\det A = 1$, and consequently, $A^{-1} = (\det A)^{-1}(\operatorname{adj} A) = A^*$, i.e., A is unitary. For $n = 2$, direct comparison of the entries of A^* and adj A gives the displayed form.

A related question is discussed in E. E. Underwood, "Classification of complex matrices A, where $A = \operatorname{adj} A$," *Current Trends in Matrix Theory*, North-Holland, 1987, pp. 405–410. Michael K. Kinyon suggested replacing (1) by the "differentiated" condition

$$A + A^* = \operatorname{tr}(A)I. \tag{2}$$

A similar method leads to the sequence of Lie algebras corresponding to the groups found above.

Solved also by D. Callan, R. J. Chapman (U.K.), I. Dimitric, W. T. Gan (student, U.K.), N.-G. Kang (student, Korea), M. K. Kinyon, N. Komanda, C. Lanski, F. Schmidt, R. Stong, E. T. Wong, University of Wyoming Problem Circle, and the proposer. Six incomplete solutions were also received.

Summing a Series of Volumes

10207 [1992, 266]. *Proposed by Eric Freden (student), Brigham Young University, Provo, UT.*

Find a closed form for $\sum_{n=0}^{\infty} \operatorname{Vol}(B^n)$ where B^n is the unit ball in $\mathbb{R}^n$ (and $\operatorname{Vol}(B^0)$ is taken to be 1).

Composite solution by several solvers. More generally, if we take $\mathbf{B}^n$ as the ball of radius r in n dimensional space, then the series converges for all $r > 0$ and

$$\sum_{n=0}^{\infty} \operatorname{Vol}(\mathbf{B}^n) = e^{\pi r^2}\left(1 + \frac{2}{\sqrt{\pi}}\int_0^{r\sqrt{\pi}} e^{-t^2}\,dt\right).$$

This is proved in detail in D. J. Smith and M. K. Vamanamurthy, "How small is the unit ball?", *Math. Magazine* 62 (1989), 101–107.

Editorial comment. Most solvers indicated a reference both for $\operatorname{Vol}(B^n)$ and the value of the resulting series. The terms of even dimension clearly determine an exponential function. The series consisting of the terms of odd degree can be recognized in terms of the solution of the initial value problem: $f'(x) = 1 + xf(x)$, $f(0) = 0$. Fourteen different references were given, none by more than three solvers.

Solved by K. F. Andersen (Canada), J. Anglesio (France), S.-J. Bang (Korea), W. H. Beckmann, D. M. Bloom, D. Callan, R. J. Chapman (U.K.), J. I. Concha (Chile), T. Dali and S. Smith and M. Carlton and P. Bracken, M. Dindos (Slovakia), M. Dresević and N. Cakić (Yugoslavia), M. Fichter (Germany), C. Georghiou (Greece), C. P. Grant, N.-G. Kang (student, Korea), M. K. Kinyon, N. Komanda, I. I. Kotlarski, R. Kreczner, O. P. Lossers (The Netherlands), S. Matz, A. Pedersen (Denmark), K. Perera (student), F. C. Rembis, R. M. Robinson, P. Sawyer (Canada), B. D. Sterba-Boatwright, R. S. Tiberio, A. Tissier (France), D. B. Tyler, D. C. Vella, M. Vowe (Switzerland), D. M. Wells, P. J. Zweir, National Security Agency Problems Group, Shreveport Problem Solving Group (LSU), University of Wyoming Problem Circle, and the proposer. One incorrect solution was received.

Answer to Picture Puzzle

(p. 847)

Louis de Branges, the solver of the Bieberbach conjecture.

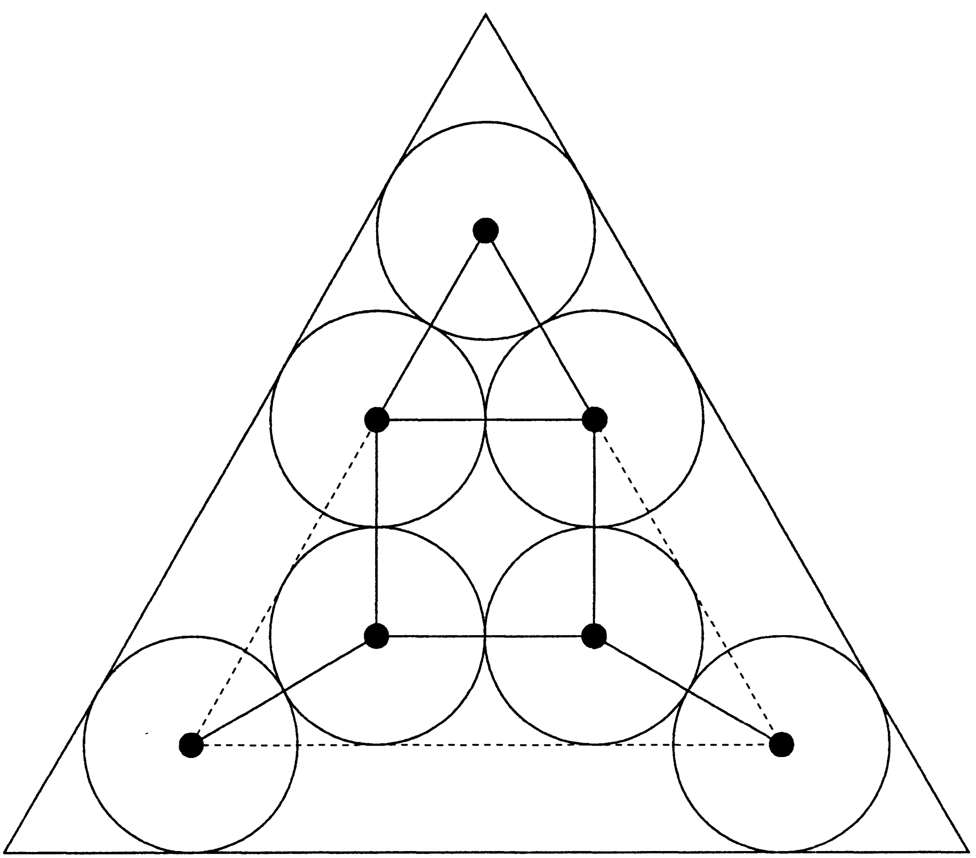
During the last quarter of a century there has been a universal effort to improve the quality of teaching in the elementary and secondary schools. Whenever a change is made in this country in the curricula for the training of teachers, it has been in the direction of more "education", pedagogy and psychology, always at the expense of further courses in subject matter. The results are already apparent; for grade schools the new method is an improvement, but for high schools, especially the last two years, it is lamentably deficient. However desirable the other things may be in themselves, for a teacher of mathematics nothing has yet been discovered to replace a knowledge of mathematics. May the present volume take its place in American and English schools, to extend the service it has so admirably rendered in Germany.

VIRGIL SNYDER

—*American Mathematical Monthly* 40 (1993), *p.* 171

The American Mathematical Monthly

Volume 100, Number 10 / DECEMBER 1993



NOTICE TO AUTHORS

The *Monthly* publishes articles, notes, and other features about mathematics and the profession. The readership of the *Monthly* is intended to include everybody who is mathematically inclined, including of course professional mathematicians and students of mathematics at all collegiate levels. While no single article or feature is likely to appeal to everyone, material should interest and be accessible to a large number of readers. This is the most important criterion for acceptance.

Articles may be expositions of old results or presentations of new ones. They may concern all of mathematics or one small area, a broad development or a single application, historical reminiscences or one important event. While some articles may contain the author's new research, the novelty of material and generality of the results is far less important than the clarity of exposition and general interest. Discussing one illuminating case of a well known result is far better than providing all the details of an obscure but new proposition. Articles in the *Monthly* are supposed to inform and to entertain; they are meant to be read rather than archived.

Notes are short and possibly informal articles. A note may concern a clever new proof of an old theorem, a novel way to present tired material, or a lively discussion of a philosophical (but still mathematical) issue. Also, any topic is suitable, so long as it is related to mathematics. Because a note is short, the first few sentences are the most important part: They should explain the purpose and invite the reader in. Photographs or diagrams often will attract the reader's attention.

All articles and notes should be sent to the editor:

JOHN EWING
Department of Mathematics
Indiana University
Bloomington, IN 47405

Please send 3 copies, typewritten on only one side of the paper. Illustrations should be carefully drawn on separate sheets of paper in black ink; the original should be without lettering and two copies should have appropriate captions and lettering indicated.

Proposed problems or solutions should be sent to:

RICHARD BUMBY,
P.O. Box 10971
New Brunswick, NJ 08906-0971.

Please send 2 copies of all material, typewritten if possible.

Letters to the Editor, both for publication and for private reading, should be sent to the Editor at the address given above. Comments, including criticisms, are welcome, as are all suggestions for making the *Monthly* a lively, entertaining, and informative journal.

Reprint permission:
MARCIA P. SWARD, Executive Director

Advertising Correspondence:
Ms. ELAINE PEDREIRA, Advertising Manager

Subscription correspondence, change of address, and other inquiries:
Membership / Subscriptions Department

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036.

Microfilm Editions: University Microfilms International, Serial Bid coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

The AMERICAN MATHEMATICAL MONTHLY (ISSN 0002-9890) is published monthly except bimonthly June-July and August-September by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, DC 20036 and Montpelier, VT. Second class postage paid at Washington, DC, and additional mailing offices. ***Postmaster***: Send address changes to the American Mathematical Monthly, Membership / Subscription Department, MAA, 1529 Eighteenth Street, N.W., Washington, DC, 20036-1385.

The American
Mathematical Monthly

Volume 100 Number 10 / DECEMBER 1993
(ISSN 0002-9890)

Contents

ARTICLES

FEATURES

Thomas Archer Hirst—
Mathematician Xtravagant
VI. Years of Decline

J. Helen Gardner and Robin J. Wilson

> I have had several letters during the week from Cayley on Geometrical Transformation. I wish I were at liberty to do my part in the important investigations that are now ripe; but I have to exercise self-denial. My lectures absorb my time and constitute my duty. Sylvester again is actively thinking and producing, and Chasles has just published a most important extension of his method. I must simply look on.

By 1865, Thomas Hirst was at the height of his powers. As Professor of Mathematical Physics at University College, London, Vice-President of the newly-formed London Mathematical Society, a member of the distinguished X-club, and a Council member of the Royal Society, he was in a position to influence those around him. A long-standing ambition was to propose the French geometer Michel Chasles for the Royal Society's Copley medal.

> **29th October 1865:** ... my proposition (although late) was well received; it was unanimously agreed that his name should be put on the list. The adjudication is on Thursday next, and I shall work hard to carry him. He has formidable rivals however in Regnault, Plücker, and Poncelet.

And he was successful, although the ailing and elderly Chasles was too unwell to come to London for the ceremony. At the celebration dinner afterwards, a toast was proposed to Chasles, the Copley Medallist and 'his friend Dr Hirst'. Following this toast, Hirst made a speech describing Chasles's achievements, which he included in full in his diary entry. He was obviously very pleased with his success, and now looked forward to presenting Chasles with his prize.

> **30th November 1865:** ... I have but one step more to take and that will be across the channel to the Passage St. Marie, Rue de Bac at Paris, there with my own hands I will place the medal in the hands of Chasles, as a grateful offering to the man who, next to Steiner, has been most influential in determining my own career.

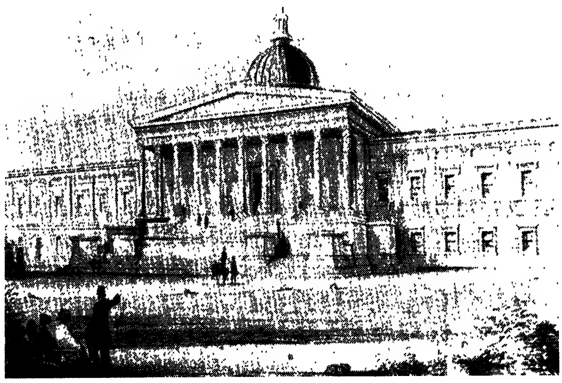
> **24th December 1865:** ... My first act this morning was to call on Chasles and deliver the Copley Medal. It was manifestly a welcome present to him ...

Throughout 1866, Hirst added further to his list of personal achievements. In February, he was elected a Member of the Athenaeum Club, in June he was appointed General Secretary of the British Association for the Advancement of Science, an onerous post which he held for four years, and in November he was admitted a Fellow of the Royal Astronomical Society. While attending a rather uninteresting meeting of one of his clubs, he 'made a calculation to show that there would be ample standing room for all the inhabitants of the Globe in the Isle of Wight'—a result which greatly surprised him.

Meanwhile, the London Mathematical Society was quickly becoming established. At one meeting, the President, Augustus De Morgan, 'called attention to the novelty and importance of many of the papers, and remarked that this was the only society in England where such papers could be received'. It seems that the Society was keen to encourage young talent:

22nd November 1866: At Math. Society. Clifford of Trin. Coll. Cambridge made his first appearance and gave us a very good paper 'on Harmonics'. There is no young mathematician of greater promise than Clifford just now.

University College, London.



In 1867 Augustus De Morgan had a disagreement with University College, and resigned his Chair in Mathematics. Hirst was elected in his place 'unconditionally and most unanimously'. He proved to be a first-class choice, if the memory of one of his students is accurate.

Thomas Hirst in 1866.

'His presence in the classroom was striking. He was tall, and held himself erect with an almost military air. He had a long black beard and a great, bald, dome-like forehead. He was a man with whom it was impossible to imagine the most audacious student venturing to take a liberty. There was something about him that invested his unlovely subject with dignity, if not interest. Less, perhaps, than any of the other professors, did he seem to think of examinations. To him, I believe, incredible as it sounds, mathematics must have been a solemn, high pursuit: a passion, if not a religion. Yet with all his aloofness of manner he could be very simple, very patient, and extremely kind. Certainly to one of his most hopeless pupils he showed himself all three.'

Meanwhile, the X-club continued its tradition of monthly meetings, with the occasional distinguished guest in attendance.

3rd March 1868: At the X-Club. Darwin was our guest. I was in the chair, and again the evening passed very pleasantly away.

2nd April 1868: At the X. Huxley, Frankland, Sir J. Lubbock and myself were the only ones who dined. Spottiswoode was there for an hour and brought Clifford with him. Clifford is the Lion of this season. Everybody is anxious to entertain him. I hope only his head will remain unturned.

But increasingly he found that his administrative and lecturing duties left him too little time for his researches, and he frequently complains of his inability to spend enough time on geometry.

7th February 1869: At home writing paper on Degenerate Conics. This paper perplexes me sorely, I begin to fear that it will never be satisfactorily written until I can work at it uninterruptedly. My daily duties so absorb my thoughts that I can only in leisure hours succeed in turning them to this new work, and no sooner are they turned and effective work rendered possible than the said duties turn them away again.

Tyndall, generous friend, proposed a remedy for this incessant disappointment I experience which I must record; it was so characteristic. "Give up your Professorship and devote yourself for a few years to your work solely. I have more money than I want and I can easily spare you what you would require to enable you to work without embarrassment."

However dear to me the privilege of thus working I could not, of course, accept it on these easy terms. My first duty is to earn my bread by teaching; if original research is not compatible with the performance of this duty then I must sacrifice originality however dear to me it may be, or however much my science might be advanced thereby. If the mathematical world prefer my teaching to my researches what right have I to complain? Can I even say that its choice is a bad one? I doubt it.

Tyndall realized that Hirst's researches could lead to important discoveries. Indeed, had he managed to persuade Hirst to take up his offer, Hirst's name might have been better remembered. As it was, the situation did not improve, and two days after his 39th birthday, Hirst wrote:

24th April 1869: Working at quadtic transformation. Cayley and Clifford have begun to work at the subject and unless I communicate what I did in 1865 I shall be out-run. How I long to have leisure to pursue my work. So long as my present drudging continues I shall be scientifically speaking extinguished.

Despite this, or perhaps because of a need for relaxation from the pressure he was under, Hirst made one of his regular visits to the Continent to meet old and new acquaintances:

26th July 1869: Bath in Neckar. We walked up to the Castle and saw all over it, the Fass included. Dined at Hotel Schrieder at 1. P.M. with Bunsen where we met Kirchhoff (on crutches) and Königsberger the Mathematician and successor of Hesse, now at Munich. We took our Abendessen with Helmholtz...

27th July 1869: After another bath in the Neckar I attended Königsberger's lecture on Theory of Determinants. He introduced me to a young Russian lady [Sonya Kowalevskaya]... who attends his lectures and is at home in Elliptic Functions. She belongs to the mathematically gifted family of Schuberts. She is pretty and exceedingly modest.

Back in England, Thomas Hirst's teaching activities took a new direction:

> Ladies' Educational Association, London. A Course of Twenty-four Lectures on the Elements of Geometry will be given by Professor Hirst, in the Minor Hall, St. George's Hall, Langham Place, on Mondays and Fridays at 11. A.M. (beginning on January 17), should a sufficient number of tickets be applied for before Christmas. The Lectures will be of an elementary character requiring no previous knowledge of the subject, the extent to which it will ultimately be carried being dependent upon the progress of the class.
>
> Fee for the Course of 24 Lectures, £11.1.6; Governesses £1.1s. Ladies over seventeen years of age may join this or any other Course in connection with the Association (that of Chemistry subject to the approval of the lecturing professor) after Christmas on the above reduced terms.

Thirty ladies enrolled for the first lecture, but about sixty attended. By the following week, fifty-seven students had enrolled, and a measure of Hirst's exceptional teaching skills may be gained in that half-way through the course he records that "one or two only have confessed inability to follow".

After long deliberation, he made up his mind to resign his chair, and apply for a well-paid administrative job which he hoped would give him more time for his research.

> **28th February 1870:** ... The fact that I cannot at present do any original work, that it is only by devoting myself wholly to lecturing that I can keep up my number of students at the College and thus secure my bread; that as my strength fails my prospects will necessarily be worse at University College; these facts I say decided me at length to apply for an appointment of an inferior order, perhaps, but of a less arduous and more remunerative character. Moreover if I succeed I shall come in contact with good and influential men and myself be able to influence to some extent the character of Education in England.

After some confusion, in March 1870 the Senate of the University of London appointed him Assistant Registrar and, for a time, his researches began to make progress again. He began work on a memoir on the "Correlation of two Planes".

> **31st December 1871:** ... It grows under my hands both in bulk and, I think, in value. Small as is my year's achievement, it has given to my life a purpose for which I feel grateful. It has raised my life in my own estimation,—and it is almost the only thing that has done so—above mere routine and mediocrity. To keep my brain clear and in a condition to discover geometrical relations has become to me a main purpose in life, all other objects have in comparison become of little moment to me.

Hirst now found time to devote to a topic which had been dear to his heart for several years. Already by 1868 he had come to believe that Euclid's *Elements* should be supplanted as the main geometry textbook in English schools, and accordingly he had spent some time editing a new geometry book by Richard Wright. This conviction, arising from his years as a surveyor and his experience of teaching practical geometry at Queenwood and University College School, left him well placed to help establish a new association whose aim was to reform the teaching of geometry in schools. This was the Association for the Improvement of Geometrical Teaching, which was founded in January 1871; Hirst was its first president, and held office for seven years. Later, in the 1880s, it broadened its scope to cover the whole range of school mathematics, and in 1897 it was re-named the Mathematical Association, a name which it holds to this day.

In 1872, Hirst was elected President of the London Mathematical Society for a period of two years. Sylvester had suggested Cayley for this post, and Hirst was also proposed, despite wanting to remain Treasurer.

The Royal Naval College in Greenwich.

10th October 1872: ... At the first vote Cayley stood first, I next and Henrici last but none obtained an absolute majority of votes. Henrici's name was accordingly withdrawn and the voting resumed when I obtained one more vote than Cayley. I voted for Cayley both times... Had Spottiswoode not strongly urged my accepting the office of President and had it been any other than Sylvester who divided the Council between Cayley and myself I should have persisted in declining to serve in any other capacity than that of Treasurer. Sylvester's *animus* against me was disagreeably manifest. It has lasted now for years and the cause of it is just as unknown to me as it was on its first appearance. ...

In the following year, Hirst embarked on his fourth (and final) career. He was appointed the first Director of Studies at the Royal Naval College in Greenwich, with a salary of £1200 per year, plus a house. This position enabled him to keep in touch with the international mathematical community.

3rd October 1873: Tchebichef, who called on me a few days ago, and Klein dined with me at Greenwich. Tchebichef told us of a mode of converting circular into rectilineal motion (á propos of the parallelogram of Watt) which was a simple and beautiful application of Quadric Inversion.

For some years there had been a lack of contact between Hirst and Sylvester. In 1875, on learning that the latter was suffering from rheumatism in the eyes, Hirst broke the long silence by expressing his sorrow at Sylvester's affliction.

25th May 1875: ... He voluntarily shook hands with me, and thus at last there is a kind of reconciliation between us. I am very glad of it, though I have learned to my sorrow that our former intimacy can never be renewed. What the exact cause of our original estrangement was I never knew, but I do know that he suspected me most unjustly of incessantly plotting to undermine his influence in the scientific and mathematical circles. He misconstrued every act and word of mine to such an extent that intercourse was impossible.

In 1878, his work was recognized by the University of Cambridge:

8th June 1878: I received the Diploma of Membership of the Cambridge Philosophical Society. I was gratified about a month ago to hear through Glaisher of my election. I may say that this is the first recognition I have ever received from any University in my native country.

The next year, he made yet another visit to the Continent. While in Paris, he met Liouville in the street.

18th May 1879: ... A little shrivelled gouty old man he has become and very garrulous. It was with difficulty I broke away from him...

More enjoyable was a visit to Parpan in Switzerland, a little Alpine village 4,545 feet above the sea, where 'I found Cremona, Casorati, Beltrami (with the Signora C), Geiser, Schläffli, Frobenius and Meier (seven mathematicians!)'.

Then, in late 1880, he learned that his unpublished researches had indeed been out-run, as he had forecast in 1869.

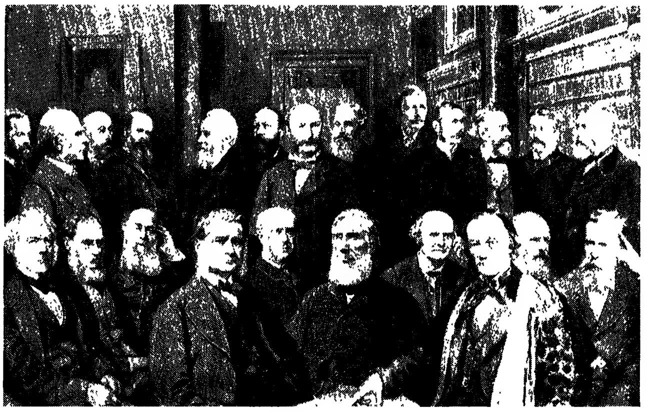
11th November 1880: The first meeting of the Math. Soc. took place on Nov. 11th. Cayley came to it and stopped with me. We were speaking of Cantor's paper on the cyclical self-corresponding points in two coincident planes between which a quadric relation exists. It has just appeared in the Annale di Matematica. I communicated precisely the same theorem to the British Association at Birmingham in 1865 but nothing was printed about it except the barest notice in the Proceedings. I showed Cayley my M.S. notes for that communication. He took them home with him and expressed an intention to write something about the matter. I shall be glad to be associated with a theorem which was always a pet of mine. As usual however I went on nursing my pet with the intention of allowing it to grow and develop itself more before I published it.

In 1883 he heard from Thomas Huxley that the Royal Society had awarded him its prestigious Royal Medal, principally for his work on Cremona transformations:

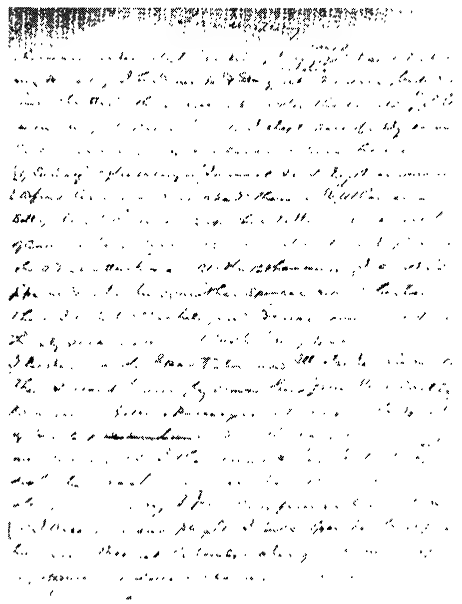
30th November 1883: ... I received my Royal Medal from Huxley who addressed to me a few friendly words in addition to the formal ones of presentation. "Although quite out of order" he said "I cannot refrain from expressing my sincere pleasure at being able, on the first occasion of my official representation of the Royal Society, to hand this Royal Medal to one of my oldest friends".

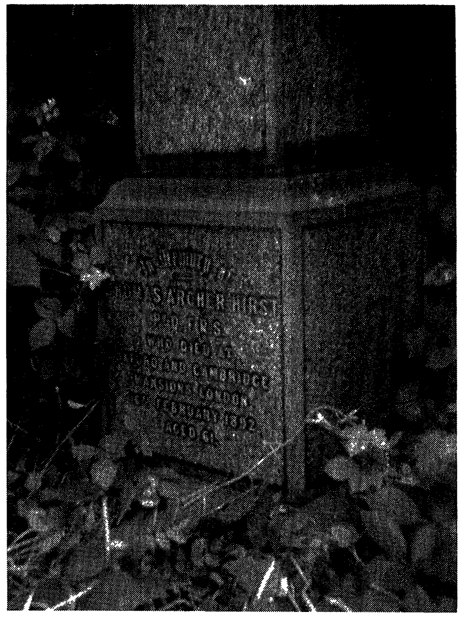
The Royal Society—a portrait group of some of the most distinguished Fellows in 1889.

At the front are, from left to right, Sir Gabriel Stokes, Sir Joseph Hooker, James Joseph Sylvester, Thomas Huxley, Archibald Geikie, John Tyndall, Arthur Cayley, Sir Richard Owen, W. H. Flower, and William Crookes.



The last entries of Hirst's diary, and Hirst's grave in Highgate Cemetery, North London.





Hirst's health had always been a cause of concern, and now it continued to decline as first kidney stones and then a stomach tumour were diagnosed. He found life very lonely when his brother John died and his favourite niece, who at one stage had been his housekeeper, married and then died in childbirth. He travelled to Greece and Egypt and in 1883 he gave up his Greenwich post at the age of 53. He now had the time to work on his geometry, at his clubs in London during the summer, and in France during the winter. He also featured in a popular book:

11th January 1890: I gave some final touches today to the notice of myself and my work in "Men of the Time". It will be posted tomorrow.

Finally, in 1890, he finished his memoir on the correlation of two spaces. He had worked on it for a long time, and after its completion he destroyed his mathematical notebooks. Suddenly he seemed old, spending his time in watching the rapidly changing world from his clubs, his flat, and the park:

23rd August 1890: ... What a mad world it is! In the distance the Sunday Band was playing unmelodiously. What a noisy, jigging world it has become!

He became increasingly depressed by the number of his colleagues and acquaintances who were departing this world.

19th February 1891: ... At the Athenaeum I read, in Nature, of the death of Madame Sophie Kovalevsky (aged 38), Professor of Mathematics at the Högskola of Stockholm. When she was 18 years of age I was introduced to her by Königsberger at Heidelberg, whose lectures she was then attending. Some years afterwards she studied under Weierstrass at Berlin... As far as her

mathematical abilities were concerned, she appears to have been superior to any predecessor of her own sex. She died from an attack of pleurisy; brought on, it is believed, by a chill which succeeded her rapid journey home from the South of France in order to commence her lectures at Stockholm.

For thirty-four years Anna had never been far from his thoughts and in September 1891, he paid one of his regular visits to Paris to bid Anna good-bye for the last time. The turn of the year brought yet more sad news.

7th January 1892: I hear from Sturm this morning that Heinrich Schröter, of Breslau, is dead. He and I heard Steiner's lectures together, at Berlin, in 1851–2... He has been taken before me. When will my time come?...

It came sooner than he thought. London was hit by a flu epidemic, one of the worst of the century. His resistance lowered by years of illness, and now suffering from cancer of the prostate, Hirst quickly succumbed. His last diary entries were written just four weeks before his death.

17th January 1892: ... the symptoms of violent cold in the head continued until nearly midnight. I then went to bed, but slept only in a disturbed fashion and awoke with pains and cramps all over my body. I fear the influenza has overtaken me.

18th January 1892: I rose in a sad plight. I took coffee for breakfast, however. This set the bowels acting; but no relief from my oppressive malaise followed. Cranstone called to look at the fallen chimney-piece in my sitting room.

On 16th February 1892 he died, and was buried in Highgate Cemetery.

Thomas Archer Hirst—Principal publications

1. On the existence of a magnetic medium, *Proc. Roy. Soc.* 7 (1854/5), 448–454.
2. On equally attracting bodies, *Phil. Mag.* 13 (1857), 305–324.
3. On equally attracting surfaces, *Phil. Mag.* 16 (1858), 160–177, 266–284.
4. On derived surfaces, *Quart. J. Pure Appl. Math.* 3 (1860), 210–218.
5. On ripples and their relation to the velocities of currents, *Phil. Mag.* 21, (1861), 188–198.
6. On the volumes of pedal surfaces, *Phil. Trans.* 153 (1863), 13–32.
7. On the quadric inversion of plane curves, *Proc. Roy. Soc.* 14 (1865), 91–106.
8. On the degenerate forms of conics, *Proc. London Math. Soc.* 2 (1866/9), 166–173.
9. On the correlation of two planes, *Proc. London Math. Soc.* 5 (1873/74), 40–70.
10. On correlation in space, *Proc. London Math. Soc.* 6 (1874/5), 7–9.
11. Notes on the correlation of two planes, *Proc. London Math. Soc.* 8 (1876/7), 262–273.
12. Note on the complexes generated by two correlative planes, *Proc. London Math. Soc.* 10 (1878/9), 131–153.
13. On quadric transformation, *Quart. J. Math.* 17 (1881), 301–311.
14. On Cremonian congruences, *Proc. London Math. Soc.* 14 (1882/3), 259–301.
15. On congruences of the third order and class, *Proc. London Math. Soc.* 16 (1884/5), 232–237.
16. On the Cremonian congruences which are contained in a linear complex, *Proc. London Math. Soc.* 17 (1885/6), 287–296.
17. Translation of R. J. E. Clausius, *The mechanical theory of heat with its applications to the steam engine and to the physical properties of bodies*, London, 1887.
18. On the correlation of two spaces, each of three dimensions, *Proc. London Math. Soc.* 21 (1889/90), 92–118.

ACKNOWLEDGMENTS. A typed version of the Thomas Hirst diaries is held at the Royal Institution in London, and quotations from the diaries appear here by courtesy of the Royal Institution. The diaries have been edited by W. H. Brock and R. M. MacLeod, and were published in microfiche by Mansell, London, in 1980.

PICTURE CREDITS. Maps of Yorkshire and Germany and Hirst's grave, courtesy Helen Gardner; Halifax (from a 19th-century print of J. R. Smith); De Morgan, Cremona, and Hirst (profile), courtesy The London Mathematical Society; Tyndall lecturing (from *The Illustrated London News*, 14th May 1870), and the Royal Society (from *The Illustrated London News*, 12th December 1863), courtesy The Illustrated London News Picture Library; Faraday (from a 19th-century print of McGuire), courtesy The Royal Institution; Hirst (portrait), Royal Naval College, Greenwich; Marburg, the University of Marburg, and Hirst's dissertation, courtesy Picture Archive, Philipps University of Marburg, Germany; Bunsen (engraved from a 19th-century photograph by C. Cook); Göttingen (from H.-H. Himme, *Stich-haltige Beiträge zur Geschichte der Georgia Augusta in Göttingen*, Vandenhoeck und Ruprecht, 1987), courtesy Vandenhoeck und Ruprecht; Berlin (from D. Botting, *Humboldt and the cosmos*, Sphere Books, 1973); Gauss (from A. Von Schwiger-Lerchenfeld, *Atlas der Himmelskünde*, 1898); Queenwood (from *The Graphic*, 25th December 1880); Liouville (from *Scripta mathematica*, 1936); Collège de France (from a postcard of around 1920); Bertrand, courtesy Archives de l'Académie des Sciences de Paris; Brioschi (from *Acta mathematica*, 1912), courtesy Mittag-Leffler Institute, Stockholm; Cayley (from *Nature*, 20th September 1883) courtesy MacMillan Magazine Limited; University College (from an engraving by C. W. Radcliffe), University College School, and Hirst (seated), courtesy University College London Library, ref. College Collection; Tyndall (from *Vanity Fair*, 6th April 1872); Huxley (from *Vanity Fair*, 28th January 1871); Royal Naval College, Greenwich, The Photographic Greeting Card Co. Ltd., London; Fellows of the Royal Society (from *The Graphic*, 20th July 1889); page of Hirst's diary, courtesy Rev. Arnold Hirst; other pictures come from the collections of the Open University and the second author. While every effort has been made to secure copyright, copyright-holders who feel that their rights have been infringed should contact the second author, and a correction will appear in a later issue.

46. Proposed by H. C. WHITAKER, A. M., Ph.D., Professor of Mathematics, Manual Training School, Philadelphia, Pennsylvania.

"There was an old woman tossed up in a basket
Ninety times as high as the moon."

Mother Goose

Neglecting the resistance of the air, how long did it take the old lady to go up?

American Mathematical Monthly
3, (1896) p. 281

Densest Packings of Congruent Circles in an Equilateral Triangle

Hans (J. B. M.) Melissen

1. INTRODUCTION. How large is the smallest square box that can contain n milk-bottles? If n points are distributed in a circle such that the distance between any two points is at least d, what is the largest possible value for d? Figure 1 shows why such problems are closely related. If K is a circular disc, or a polygonal region whose edges are all tangent to a circle, packing n equal circular discs of maximum diameter inside K is equivalent to finding n points in K such that the pairwise minimum distance between points is maximal. For instance, in a unilateral triangle, these points are the centers of circles of diameter d that pack into $(1 + \sqrt{3}\,d)K$. We will refer to d as the *maximum separation distance* of n points in K. As there seems to be little hope of solving the packing problem for all n, research has been focussed on asymptotic estimates and on the investigation of small values of n.

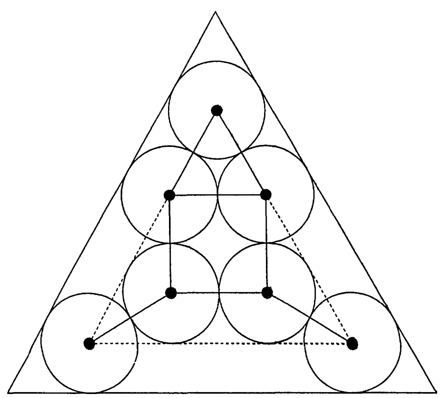


Figure 1. Densest packing of seven circles in an equilateral triangle. Seven points in an equilateral triangle with largest possible minimum distance between the points.

During the last decades much progress has been made for circle packings inside a number of simple geometrical shapes, such as the square and the circle. Solutions were found by trial and error or by computer aided optimization. Although near-optimal packings are easy to construct, few optimality proofs have appeared so far and many conjectures still rest unproven. An excellent review with relevant references can be found in **[2]**; see also **[4, 11]**.

In 1969 Pirl **[13]** exhibited circle packings in a circle for $n = 2, \dots, 20$ and proved their optimality for $n \leq 10$. A proof for $n = 11$ was given recently by the author **[8]**.

Optimal circle packings in a square have been constructed for $n = 6$ by Graham, for $n = 7$ by Schaer (both unpublished), for $n = 8$ by Schaer and Meir **[14]** and for $n = 9$ by Schaer **[15]**. Wengerodt (and Kirchner) **[18, 17, 19, 7]** gave proofs for $n = 14, 16, 25$ and $n = 36$.

Another problem that comes to mind is the packing of equal circles into an equilateral triangle. Surprisingly, only the case of the triangular numbers $n = k(k+1)/2$ has been tackled in the literature **[12, 2]**. In the vein of Pirl, Schaer and Wengerodt we will provide optimal arrangements for $n \leq 10$, $n = 12$ and give an alternative proof for the triangular numbers.

The closely related problem of partitioning an equilateral triangle into subregions such that the maximum of the diameters is minimal has been studied by Graham **[6]**. Optimal packings of 2, 3, 4, 5, 8, 9 and 10 equal spheres in a regular tetrahedron can be found in **[1]**.

2. OPTIMAL PACKINGS IN AN EQUILATERAL TRIANGLE. Figures 2a–k and 2p show arrangements of n points inside a unilateral triangle for which the minimum distance between the points is maximal. The solid lines in the figures connect those pairs of points for which the distance is equal to the maximum separation distance d_n. The values of d_n are given in Table 1. For $n = 2, 3, \ldots, 10, 12$ we will prove that the arrangements shown are indeed optimal. The proofs for $n = 2, \ldots, 7, 10$ consist in constructing a decomposition of the triangle into at most $n - 1$ subregions. Dirichlet's pigeon-hole principle tells us that one of the subregions must contain at least two points. The maximum diameter of the subregions is then an upper bound for the minimum possible distance between two points of the arrangement. In the cases under consideration, this upper bound is attained by the given configuration. The optimality proof for the arrangements of eleven points is rather involved and will be the subject of a separate paper. The cases $n = 2, 3$ are evident, so we will proceed with $n = 4$.

2.1. Arrangement of Four, Five and Six Points. Two of the four points must lie in the same subregion from the partition shown in Figure 3a, so $d_4 \leq 1/\sqrt{3}$. If the upper bound is attained, then one point must lie at the center and the other one is a vertex of the triangle. The only possible locations left for the other two points are then the other two vertices of the triangle, so for $n = 4$ the configuration is unique.

Using the partition of the triangle into four triangles as in Figure 2e, it follows that the maximum separation distance for $n = 5$ and $n = 6$ is equal to $1/2$. The configuration for $n = 5$ is just the arrangement for $n = 6$ from which one arbitrary point has been removed. This is the only freedom allowed in finding an optimal arrangement for $n = 5$.

2.2. Arrangements of Seven Points. An interesting feature of $n = 7$ is that, apart from reflected configurations, there are two different types of optimal solutions as is illustrated in Figures 1 and 2f. One is symmetric and rigid. In the other one (dashed in Figure 2f), where the interior point on the left is moved to the base of the triangle, the position of the left point in the second row is no longer unique. By projecting on the base of the triangle it can be seen from the configuration in Figure 2f that its separation distance is equal to $d_7 = (\sqrt{3} - 1)/2$. The partition shown in Figure 3b is based on the points that lie on the edges and on the bisectors of the triangle, and that are at distance d_7 from the vertices, together with the center of the triangle. From this partition it follows immediately that the maximum

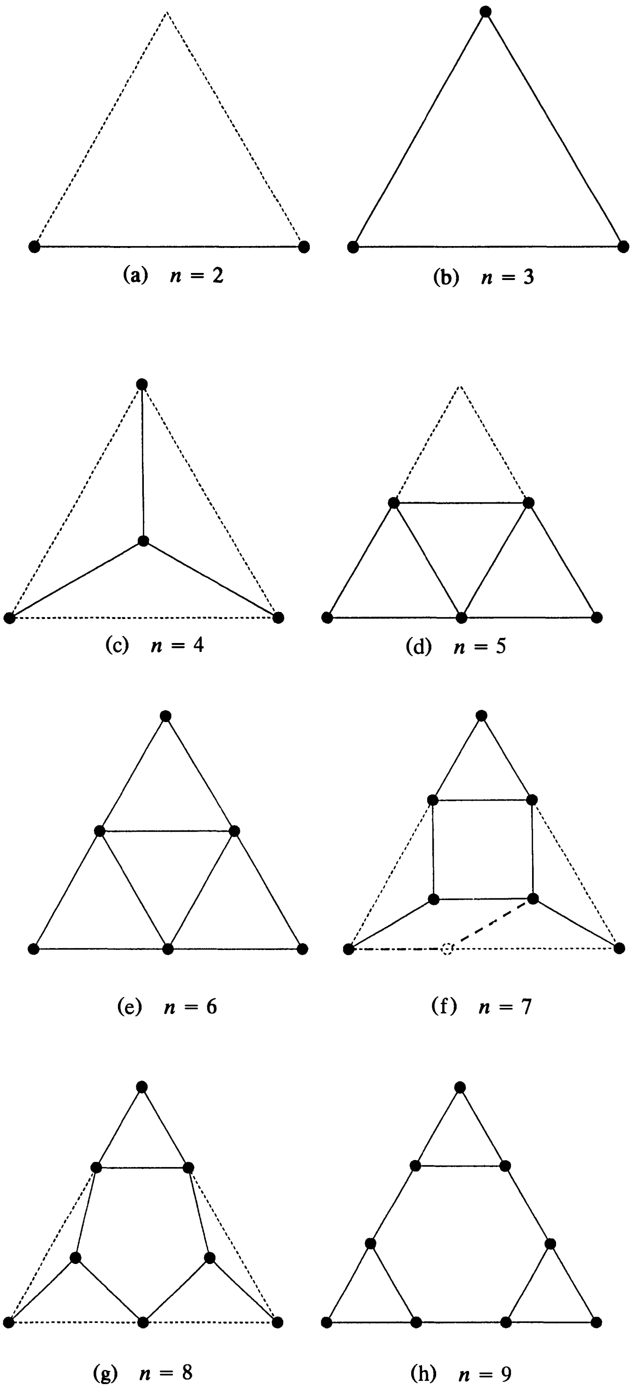


Figure 2. Optimal and conjectured optimal (*) arrangements of points in a unilateral triangle. The solid line segments are of length d_n.

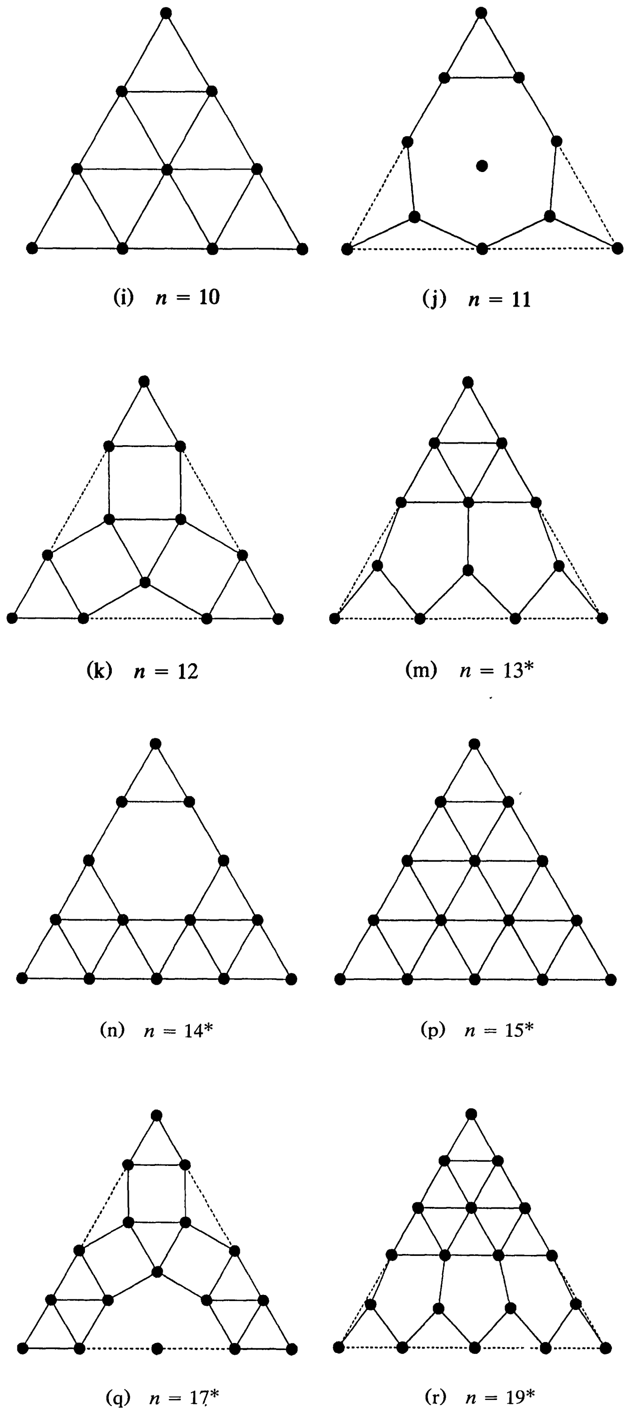


Figure 2. (*Continued*).

TABLE 1. Maximum separation distance d_n of n points in a unilateral triangle

n	max. separ. distance d_n		n	max. separ. distance d_n	
2, 3	1	= 1.000000...	12	$2-\sqrt{3}$	= 0.267949...
4	$1/\sqrt{3}$	= 0.577350...	13*		= 0.251813...
5, 6	$1/2$	= 0.500000...	14*, 15	$1/4$	= 0.250000...
7	$(\sqrt{3}-1)/2$	= 0.366025...	17*	$(3-\sqrt{3})/6$	= 0.211324...
8	$(\sqrt{33}-3)/8$	= 0.343070...	19*		= 0.200321...
9, 10	$1/3$	= 0.333333...	$k(k+1)/2-1$*	$1/(k-1)$	
11	$(3-\sqrt{6})/2$	= 0.275255...	$k(k+1)/2$	$1/(k-1)$	

*marks the conjectured values.

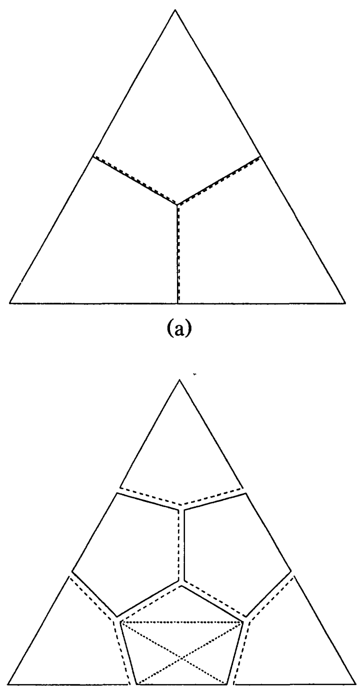

(a)
(b)

Figure 3. Partitions for $n = 4$ and $n = 7$. The solid lines indicate to which subregion each edge belongs. The three dotted lines in (b) are of length d_7.

separation distance is equal to d_7. The pentagonal regions can contain at most two points at distance d_7, in exactly one way, whereas the quadrilateral regions can accommodate only one point. Easy combinatorial arguments show that only the configurations described above are possible.

2.3. Arrangements of Eight Points. A straightforward computation shows that the separation distance for the configuration in Figure 2g satisfies an equation of degree four, leading to a separation distance of $d_8 = (\sqrt{33} - 3)/8$. The arrangement is unique up to rotations.

To prove that d_8 is optimal, suppose that we have a configuration for which the distance between any two points is at least $d > d_8$. It is easy to see that a point that is closest to a vertex of the triangle can be moved to that vertex without

disturbing the optimality of the solution. We can therefore assume that the three vertices of the triangle are part of the configuration. This assumption will not restrict the total number of solutions to be found.

We will make use of the decomposition in Figure 4a. The vertices in this partition can be found by using the points from the arrangement in Figure 2g and their rotated images, together with the center of the triangle. Consider the closed region formed by the union of the subregions $R_1, R_2, R_3, Q_1, Q_2, Q_3$. In this region five points must be accommodated at a mutual distance of at least d. All its subregions have a diameter of at most d_8. As $d_8 < d$, each cannot hold more than one point of the solution. This means that two of the Q_j, together with their interjacent R-region must each contain one point of the solution, for instance Q_1, R_1, Q_2. This cannot happen, because $|A_3D| = |B_3D| = d_8$. Here D is the midpoint of A_1B_1 (divide $Q_1 \cup R_1 \cup Q_2$ with a cut along DC and apply the pigeon-hole principle).

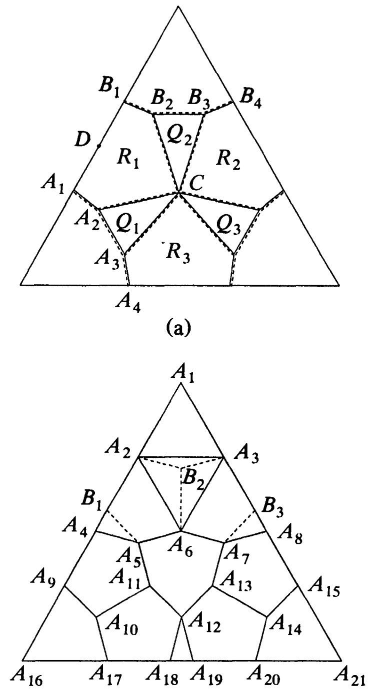


Figure 4. Partitions for $n = 8$ and $n = 12$.

Now we shall determine all possible configurations for which the separation distance is equal to d_8. Each $\overline{R}_j$ (the closure of R_j) can contain at most two points of the solution. For instance, for $\overline{R}_1$, the possible combinations would be $A_1 - B_2$ and $A_2 - B_1$. First, we show that no Q_j can contain a point of the solution in its interior.

1. If two of the Q-regions, for instance Q_1 and Q_2, have a point of the solution in their interior, then $\overline{R}_1$ cannot contain a point. Furthermore no point can be in the interior of Q_3, otherwise there could be no solution points in $\overline{R}_2$ and $\overline{R}_3$. This

implies that the union of $\bar{R}_2$ and $\bar{R}_3$ must contain at least three points of the solution, so one must contain two points. This is impossible, because one of these points (A_3, A_4, B_3 or B_4) would then be too close to at least one of the solution points in Q_1 or Q_2.

2. If only Q_1 has a solution point in its interior, then $\bar{R}_1$ and $\bar{R}_3$ will not contain more than one point each, so there must be two points in $\bar{R}_2$. This cannot occur because one of these points would be too close to the points of the configuration in $\bar{R}_1$ and $\bar{R}_3$.

The five points must therefore be distributed over $\bar{R}_1, \bar{R}_2, \bar{R}_3$. As the center of the triangle cannot be part of the solution, one of the three regions (e.g. $\bar{R}_3$) contains only one point. This implies the solution given in Figure 2g. The arrangement is unique up to rotations.

2.4. Arrangements of Nine and Ten Points. The unique configuration for $n = 10$ is an easy consequence of the pigeon-hole principle, applied to the obvious subdivision into triangles (see Figure 2i). The configurations for $n = 9$ can be obtained by removing one arbitrary point from the arrangement for $n = 10$. Unfortunately the pigeon-hole principle cannot be applied, because a partition into eight regions must contain a subregion of diameter $2/(1 + \sqrt{3} + \sqrt{6\sqrt{3}}\,) > 1/3$ ([**6**]).

First, we shall demonstrate that the maximum separation distance for $n = 9$ is equal to $1/3$. Suppose that for some configuration the distance between the points is at least $1/3 + \varepsilon$, where $\varepsilon > 0$. This means that there must be exactly one point in each subregion in Figure 2i. The three points in the three outermost triangles prohibit other points from coming within a distance ε from the edges of these triangles. Consequently, the region inside the hexagon where the remaining six points should be situated is actually contained in a disc of radius $r_0 = \sqrt{1 - 3\varepsilon + 9\varepsilon^2}\,/3 < 1/3$. According to Pirl [**13**, §2], the separation distance of these points cannot exceed r_0, which contradicts the assumption that the distance exceeds $1/3$.

Having established d_9 it is not difficult to see that all optimal arrangements for $n = 9$ can be obtained by removing one arbitrary point from the arrangement for $n = 10$. This follows from the fact that the circumscribed circle of the six innermost triangles can enclose at most seven points with a mutual distance of at least $1/3$. On the other hand, the three regions outside this circle can contain at most three points in all, so there must be at least six points in the circular disc. From the configurations for the circle found by Pirl it follows that only the vertices of the small triangles can be part of the configuration.

2.5. Arrangements of Twelve Points. The unique optimal configuration for $n = 12$ is shown in Figure 2k. Consider the partition as indicated by the solid lines in Figure 4b. The coordinates of the nodes can be found in Table 2. The subdivision is symmetric in the bisector through A_1. The triangle is now divided into twelve regions whose diameter is at most $d_{12} = 2 - \sqrt{3}$. If the maximum separation distance of an arrangement were larger than d_{12}, then there would be exactly one point in each subregion. The presence of a solution point in $A_{18}A_{19}A_{12}$ subsequently implies that there is a point in the interior of $A_{10}A_{11}A_{17}$, $A_4A_5A_{11}A_9$, $B_1A_5A_6A_2$ and of $A_2A_3B_2$, so there can be no point in $A_1A_2A_3$. This contradiction implies that d_{12} is the maximum separation distance.

Next, we will find the unique arrangement corresponding to this maximum separation distance. Arguments similar to those already discussed show that there can be no point in $A_{18}A_{19}A_{12}$ (with the possible exception of A_{12}). By symmetry

TABLE 2. Coordinates of the nodes in the partitions for $n = 12$

	x	y		x	y
A_1	0	$\frac{1}{2}\sqrt{3}$	A_{11}	$\frac{5}{2} - \frac{3}{2}\sqrt{3}$	$-\frac{3}{2} + \sqrt{3}$
A_2	$-1 + \frac{1}{2}\sqrt{3}$	$\frac{3}{2} - \frac{1}{2}\sqrt{3}$	A_{12}	0	$1 - \frac{1}{2}\sqrt{3}$
A_4	$-2 + \sqrt{3}$	$3 - \frac{3}{2}\sqrt{3}$	A_{16}	$-\frac{1}{2}$	0
A_5	$-1 + \frac{1}{2}\sqrt{3}$	$-\frac{1}{2} + \frac{1}{2}\sqrt{3}$	A_{17}	$\frac{3}{2} - \sqrt{3}$	0
A_6	0	$3 - \frac{3}{2}\sqrt{3}$	A_{18}	$-\frac{7}{2} + 2\sqrt{3}$	0
A_9	$\frac{1}{2} - \frac{1}{2}\sqrt{3}$	$-\frac{3}{2} + \sqrt{3}$	B_1	$\frac{3}{2} - \sqrt{3}$	$-3 + 2\sqrt{3}$
A_{10}	$-2 + \sqrt{3}$	$1 - \frac{1}{2}\sqrt{3}$	B_2	0	$-2 + \frac{3}{2}\sqrt{3}$

the same must be true for $A_4A_5B_1$ and $A_7A_8B_3$. Now we adapt the decomposition of the triangle to one with the three bisectors of the triangle as axes of symmetry. This is indicated by the dashed line segments in Figure 4b. The region $A_4A_5A_{11}A_{12}A_{18}A_{16}$ with the segments A_5A_{11} and $A_{11}A_{12}$ excluded can contain a maximum of four points of the optimal arrangement, and this in exactly one way ($A_4, A_{10}, A_{16}, A_{18}$). This is evident from the partition into three subregions of diameter d_{12}. The central hexagon can contain a maximum of three points (A_5, A_7, A_{12}). Straightforward combinatorial arguments then show that three solution points in the hexagonal region correspond to the arrangement in Figure 2k, whereas two or less points cannot lead to a solution.

2.6. Arrangements for Triangular Numbers. For the triangular numbers $n = k(k + 1)/2$, $(k \geq 2)$, the obvious candidates for the optimal arrangements are given by the regular triangular lattice arrangement in analogy to Figures 2b, e, i, p. Unfortunately, the partitioning trick is unsuitable to prove this for all triangular numbers. This is because the number of triangles $(k - 1)^2$ exceeds the number of points n, for $k \geq 5$. Oler **[12]** asserted that the minimum distance between $n + 1$ points in a unilateral triangle is smaller than $1/(k - 1)$. Looking at his proof we notice that Oler actually proved that $d_n = 1/(k - 1)$, however, without showing that the obvious arrangement is indeed unique. The proof is based on a general inequality that was conjectured by Zassenhaus and proved by Oler in 1961 (see **[5]**). This inequality provides an upper bound for the number of points n that can be placed in a planar convex compact set K at a mutual distance of at least 1, expressed in terms of the area $\mu(K)$ and the perimeter $\mu(\partial K)$ of K:

$$n \leq \frac{2}{\sqrt{3}}\mu(K) + \frac{1}{2}\mu(\partial K) + 1. \tag{1}$$

The optimality proof for the triangular numbers is obtained by applying this inequality to an equilateral triangle. A similar inequality of Groemer (1960, see **[10]**) can also be used. We shall give a more straightforward proof by deriving this inequality directly for the case of a unilateral triangle. In addition we can also conclude the uniqueness of the optimal solution.

Theorem. *If $n \geq 2$ points are placed inside a unilateral triangle then the minimum of the mutual distances between these points, d, satisfies the following inequality:*

$$d \leq \frac{2}{\sqrt{8n + 1} - 3}. \tag{2}$$

Equality is attained only if $n = k(k + 1)/2$, $(k \geq 2)$, for points on a regular triangular lattice.

Proof: Suppose that for some n an arrangement is given. The circles centered around these points with radius $r = d/2$ then form a packing inside an equilateral triangle with a side-length of $1 + 2\sqrt{3}\,r$. The plane could be tiled with these triangles to obtain a global circle packing. For our purpose, however, this packing is not good enough. We will use a more economical packing shown in Figures 5 and 6. The packing is reflected in a line parallel to one side of the triangle

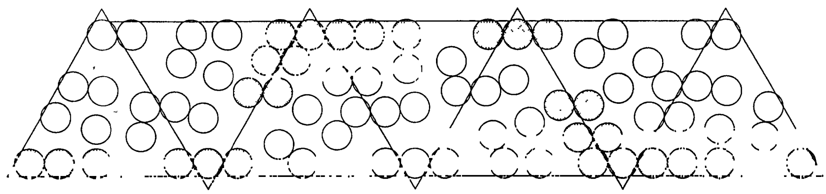


Figure 5. Packing of packed triangles in a strip.

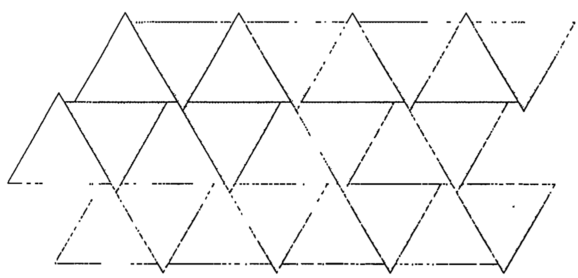


Figure 6. Tiling with truncated triangles.

touching the circles. This mirror image is then slightly moved until it fits snugly into the original arrangement (see Figure 5). It is easy to see that this can always be done. This process is repeated to obtain an infinitely long strip of circle packings. The same technique is then applied to the strip resulting in a global circle packing. This is possible because in the strip the arrangement of circles repeats itself after six triangles. The side-length of the triangles in Figure 5 is $1 + 3r$. Although these triangles overlap, the plane can be tiled by the trapezoids as shown in Figure 6 (the shaded regions correspond to mirror images of the arrangement). It is a well-known result of Thue **[16, 4]** that the density of a plane circle packing cannot exceed $\pi/\sqrt{12}$ and that this maximum value is attained for the honeycomb packing where each circle touches six neighbors and the centers are on a regular triangular lattice. This implies the following estimate:

$$\frac{n\pi r^2}{\frac{1}{4}\sqrt{3}\left[(1 + 3r)^2 - r^2\right]} \leq \frac{\pi}{2\sqrt{3}},$$

which leads to inequality (2). For triangular numbers $n = k(k + 1)/2$, this inequality reduces to $d \leq 1/(k - 1)$; in this case the hexagonal packing is the unique optimal solution. ■

3. CONJECTURES. For $n = 13, 14, 19$, conjectures for the optimal arrangements are presented in Figure 2m, n, r. The optimal arrangements for $n = k(k + 1)/2 - 1$ seem to be obtained by removing one arbitrary point from the arrangement for $n = k(k + 1)/2$. This conjecture was posed as an open problem by Erdős and Oler

[12, 2]. We have already shown its validity for $n = 2, 5, 9$. The conjecture actually implies a still open conjecture of Fejes Tóth [3], which states that if $n + 1$ circles are removed from the honeycomb packing of equal circles, and n are packed again in the resulting interstitial space, then we always end up with the original packing from which one circle has been removed.

The configurations in Figures 2c, g, m, r suggest a possible form for the optimal arrangements for $n = k(k+1)/2 - 2$, $(k \geq 3)$. First $k - 3$ layers of $(k-3)^2$ equilateral triangles, followed by a layer of $k - 3$ pentagons. We conjecture that these are the unique optimal configurations in these cases (up to rotations). The conjecture is true for $n = 4$ and 8.

Conjectures for $n = 16, 17$ and 18 are presented in [9]. One configuration is shown in Figure 2q.

Acknowledgments. I would like to thank Prof. J. H. van Lint, Dr. P. C. Schuur, Dr. A. J. E. M. Janssen and Drs. M. J. J. J. B. Maes for reading the drafts of the paper and for useful discussions.

REFERENCES

1. K. Bezdek, Densest packing of a small number of congruent spheres in polyhedra, *Ann. Univ. Sci. Budapest Eötvös Sect. Math.* **30** (1987) 177–194.
2. H. T. Croft, K. J. Falconer and R. K. Guy, *Unsolved Problems in Geometry*, Springer Verlag, Berlin, 1991, 107–111.
3. L. Fejes Tóth, Solid circle-packings and circle-coverings, *Studia Sci. Math. Hung.* **3** (1968) 401–409.
4. ______, *Lagerungen in der Ebene, auf der Kugel und im Raum*, (1953) 2^e Auflage (1972), Springer Verlag, Berlin.
5. J. H. Folkman and R. L. Graham, A packing inequality for compact convex subsets of the plane, *Canad. Math. Bull.* **12** (1969) 745–752.
6. R. L. Graham, On partitions of an equilateral triangle, *Canad. J. Math.* **19** (1967) 394–409.
7. K. Kirchner and G. Wengerodt, Die dichteste Packung von 36 Kreisen in einem Quadrat, *Beiträge Algebra Geom.* **25** (1987) 147–159.
8. J. B. M. Melissen, Densest packings of eleven congruent circles in a circle, to appear, *Geom. Dedicata.*
9. J. B. M. Melissen and P. C. Schuur, Packing 16, 17 and 18 circles in an equilateral triangle, to appear, *Discrete Math.*
10. J. Molnár, On the packing of unit circles in a convex domain, *Ann. Univ. Sci. Budapest Eötvös Sect. Math.* **22/23** (1979/80) 113–123.
11. W. O. Moser and J. Pach, *Research Problems in Discrete Geometry*, Montreal (1984).
12. N. Oler, A finite packing problem, *Canad. Math. Bull.* **4** (1961) 153–155.
13. U. Pirl, Der Mindestabstand von n in der Einheitskreisscheibe gelegenen Punkten, *Math. Nachr.* **40** (1969) 111–124.
14. J. Schaer and A. Meir, On a geometric extremum problem, *Canad. Math. Bull.* **8** (1965) 21–27.
15. J. Schaer, The densest packing of 9 circles in a square, *Canad. Math. Bull.* **8** (1965) 273–277.
16. A. Thue, Om nogle geometrisk-taltheoretiske theoremer, *Forhdl. Skand. Naturforskeres* **14** (1892) 352–355.
17. G. Wengerodt, Die dichteste Packung von 16 Kreisen in einem Quadrat, *Beiträge Algebra Geom.* **16** (1983) 173–190.
18. ______, Die dichteste Packung von 14 Kreisen in einem Quadrat, *Beiträge Algebra Geom.* **25** (1987) 25–46.
19. ______, Die dichteste Packung von 25 Kreisen in einem Quadrat, *Ann. Univ. Sci. Budapest Eötvös Sect. Math.* **30** (1987) 3–15.

Philips Research Laboratories
P.O. Box 80.000
5600 JA Eindhoven
The Netherlands
melissen@prl.philips.nl

Partnerships[1]

Alan H. Schoenfeld

In the section called "Action," *Everybody Counts* (National Research Council, 1989) issued this clarion call:

> "In the next decade, the United States has a historic opportunity to revitalize mathematics education...
>
> "There are at this time both a particular urgency and a special opportunity for reform of mathematics education. Since mathematics is the foundation of science and technology, reform is needed to prepare the more highly skilled work force that the nation now needs. Because of the emerging general agreement within the mathematics, mathematics education, and related professional communities on goals for mathematics education and means for achieving them, there is at this time a special opportunity for the nation to push ahead boldly in this area of education. (page 87)"

The mathematics education community has indeed been pushing boldly ahead, and it is of great interest to note the character of the advances—especially as they contrast with the character of the field in its early days, approximately a quarter-century ago.[2] For example, Joe Crosswhite recalls that the first research sessions at an annual NCTM meeting were held behind the stage, behind a closed curtain—placed by conference organizers at a safe physical and psychological distance from more "teacherly" conference activities. Physically and intellectually, the research community stood apart. Indeed, its apartness was manifested in multiple ways: in focus, in methods, and in the communities from which it drew. As in all of the social sciences through the 1960's and 1970's, the methods employed tended to be "rigorous" and "scientific," with a focus on experimental studies and statistical analyses. Many experiments took place in the lab, at some remove from instruction. Those studies which took place in classrooms tended to downplay the complexity of classroom interactions, focusing on specific instructional "variables" and their effects, as determined statistically. Hence in 1978 Kilpatrick felt obliged to suggest that educational researchers might have lost sight of meaningful mathematical behavior in their search for methodological rigor, and that the community might have much to learn from unrigorous but interesting studies such as the

[1]This report was prepared by Alan H. Schoenfeld, University of California at Berkeley, chair of the NCTM Research Advisory Committee, and was reviewed by members of the Committee. At the time this report was prepared in April 1993, committee members were Deborah Ball, Michigan State University; Robert Davis, Rutgers University; Beverly Ferrucci, Keene State College of New Hampshire; Marilyn Hala (Staff Liaison), NCTM Headquarters; Miriam Leiva (Board Liaison), University of North Carolina at Charlotte; Susan Jo Russell, TERC; William Tate, University of Wisconsin.

[2]Papers in mathematics education can be traced back a good many years, of course, but the creation of the *Journal for Research in Mathematics Education* about 25 years ago is generally taken as a sign of the coalescence of the discipline.

largely qualitative teaching experiments carried out in the Soviet Union by researchers such as Krutetskii (1976). In terms of communication across communities, Pólya was the exception that *probed* the rule: after the burst of energy that produced the New Math, there was little interaction between the mathematics and the math-ed communities, especially along the lines of research.

Things have changed! As noted in *Everybody Counts*, "real change requires action by everyone involved in mathematics education" (page 93). The Mathematical Sciences Education Board, formed in 1985, represents an attempt to bring together the various constituencies that have a stake in mathematics education. Multiple communities have a stake in getting things right. More importantly, multiple communities have major contributions to make.

Mathematicians, for example, live and breathe the discipline; they can offer a deep sense of what it is to engage in mathematics, and a sense of what might be called the "mathematical validity" of a curriculum—whether the ideas and processes with which students engage tend to reflect the deep underlying notions of mathematical "doing." In recent years the mathematical community's interest in educational issues has mushroomed: witness the existence of Mathematicians and Educational Reform, a grass roots organization of university mathematicians with interest in contributing to K-12 mathematics education, and the fact that the American Mathematical Society has created a Committee on Education, one major function of which is to establish liaison with other, longer-established groups with educational interests.

In many ways the teaching community has been galvanized by the *Curriculum and Evaluations Standards for School Mathematics* (NCTM, 1989) and the *Professional Standards for Teaching Mathematics* (NCTM, 1991). The wisdom of the profession was a major factor in the creation of those documents, and will be an essential resource if we are to reach to goals set forth in them: teachers live the reality of instruction in their classrooms, and must be the wellspring of the reform movement. And the professional teaching community is ready for interactions with the other communities, as evidenced by the spectacular growth in NCTM membership and attendance at annual NCTM meetings in recent years, and the diversification of conference programs to include a significant focus on research-related activities.

Beyond the classroom, schools, school districts, parental understanding and influence, state departments of education and national curricular influences (texts and tests) are major factors that affect the ways in which reform can take place, and whether it will be sustained. Members of all these communities need to be enfranchised, and need to contribute to dialogue and change.

Last but not least, the community of mathematics educators has grown spectacularly over the past 25 years, and is capable of being a central "team player" in the reform of the profession. Even a cursory glance at the *Handbook of Research on Mathematics Teaching and Learning* (Grouws, 1992) reveals how vibrant and robust an enterprise research in mathematics education has become. A closer look reveals how much the field has broadened, in the range of methods it employs and the phenomena it explores. Methods include computer simulations of individual cognition, clinical interviews, classic laboratory studies, ethnographic analyses of classroom cultures, qualitative studies of teacher and student beliefs and their effects on behaviors, and more. The classroom, once seen by most as "too complex" for careful studies of mathematical thinking and learning, is now seen by many as the natural place for such studies. Along with inward growth came an outward look: the mathematics education community now looks to teachers, mathematicians,

psychologists, cognitive scientists, anthropologists, and numerous other communities for issues, ideas, and inspiration as it seeks to grapple with the complex phenomena of mathematical understanding, thinking, and learning.

We are, then, at an important point in the development of mathematics education. There is general recognition that the problems we face are large, and that they require the concerted effort of all the major constituencies involved in the educational process. Although many of those constituencies have in the past been communities apart, there is now unprecedented potential for collaborative work and joint community building. Over the past few years, the Research Advisory Committee in particular and NCTM in general have been moving in those directions. Here are some examples of recent, proposed, and potential projects.

Two years ago (July 1991) RAC reported on the NCTM *Standards* Research Catalyst conferences, which were then in progress. One major goal of the conferences, supported by the NSF and held in March and December 1991, was to focus research on major themes in the *Curriculum and Evaluations Standards for School Mathematics*. The profession needed to know more about assessment, curriculum change, communication, policy, representational tools and models, and the changing secondary curriculum; it made sense to have focus groups address those issues. But an equally important goal was the enfranchisement of a new research community, reaching out from the traditional base of mathematics educators to teachers, administrators, and others to begin research and research partnerships in these areas. By any measure, the effort was a significant success: a number of new researchers received NSF seed grants for work stimulated by the conference, and some of the partnerships formed (e.g. the communications group) continue today as active research collaboratives.

We hope, a few years from now, to report on a similar undertaking related to the *Professional Standards for Teaching Mathematics* entitled the "Collaborative for enhancing research in mathematics teaching." The goal of the proposed collaborative is to build a community of people working together to conceptualize and carry out research on mathematics teaching, with an emphasis on broadening the kinds of research being used to inform reform efforts and exploring new ways to communicate about research to diverse audiences. The collaborative is especially interested in attracting new researchers, experienced researchers new to research on mathematics teaching, mathematicians, and mathematics educators whose activities have not traditionally been considered to be research (e.g. classroom teachers, staff developers, administrators, college teachers).

With the help of the Exxon Education Foundation, work is now under way on the first phases of a project entitled "Recognizing and recording reform in mathematics education: Documenting the effects of the National Council of Teachers of Mathematics *Curriculum and Evaluations Standards* and *Professional Standards for Teaching Mathematics*." This project, quite large in scope, is intended to take a systemic view of change, and to help the community at large understand the dynamics of educational reform. This project will, of necessity, involve all the major constituencies involved in mathematics education. From the project description: "Such a project, through its structure and intent, emphasizes that the changes outlined in the *Standards* documents will not happen quickly, or easily, or without experimentation and false starts. A project such as this confirms that it is not only acceptable, but essential, to learn from the process of implementation and change and to disseminate and share that knowledge openly, even

though the stories that emerge will describe obstacles and difficulties as well as successes."

Finally, a set of activities on "Partnerships in research" is in the planning stages. The task force working on the project expects to assemble videotapes of classroom instruction that can serve as the focal points for conversations among mathematicians, teachers, administrators, and mathematics education researchers regarding the values, goals, and practices of mathematics instruction. It hopes that first at a national conference, and then at a series of spin-off local conferences, the videotapes and related support materials will serve as means of facilitating conversations among those groups, all of which are essential for continued progress in educational reform.

These are exciting times. The spirit of reform is in the air; the communities necessary to promote it are open to collaboration; and efforts to join forces in this important collaborative enterprise are being undertaken. That the various communities listed above have grown to the point where they recognize their interdependencies and are willing to build partnerships bodes well for all concerned, and should cheer us all—but it should not leave us feeling complacent. We have just embarked on the collaborative trail, and there is much more to be done. Although one can point to exceptions in individual states and locales, the research community has not, in general, been adequately engaged with policy makers at the state and national levels. Local, state, and national policies may or may not be consistent with our best understandings. Likewise, local, state, and national assessment measures may support or may undermine what we would like to have happen in our nation's mathematics classrooms. Much more direct contact and productive interaction among the policy, assessment, and research communities is necessary. Similarly, although there are encouraging signs of interactions, the research community has yet to engage adequately with issues of teacher preparation. And, of course, this brief list of necessary collaborations can be expanded without difficulty. In sum, let us take pleasure in the progress we have made. Then, let us return to the task of making and strengthening essential partnerships for progress in mathematics education.

REFERENCES

Grouws, D. (Ed.) (1992). *Handbook of research on mathematics teaching and learning*. New York: MacMillan.

Kilpatrick, J. (1978). Variables and methodologies in research on problem solving. In L. Hatfield (Ed.), *Mathematical problem solving* (pp. 7–20). Columbus, OH: ERIC.

Krutetskii, V. A. (1976). *The psychology of mathematical abilities in school children*. (J. Teller, translator; J. Kilpatrick, & I. Wirszup, Eds.). Chicago: University of Chicago Press.

National Research Council. (1989). *Everybody counts: A report to the nation of the future of mathematics education*. Washington, DC: National Academy Press.

National Council of Teachers of Mathematics. (1989). *Curriculum and evaluation standards for school mathematics*. (Reston, VA: NCTM.

National Council of Teachers of Mathematics. (1991). *Professional standards for teaching mathematics*. Reston, VA: NCTM.

Research Advisory Committee (1991). NCTM Standards research catalyst conference. *Journal for Research in Mathematics Education*, 22(4), 293–296.

Education and Mathematics Department
University of California, Berkeley
Berkeley, CA 94720

A Simple Proof of Pascal's Hexagon Theorem

Jan van Yzeren

Pascal's Theorem. *If the vertices of a hexagon lie on a circle and the three pairs of opposite sides intersect, then the three points of intersection are collinear.*

This theorem was published in 1640 by sixteen-year-old Blaise Pascal. His original proof has been lost, and at times one wonders whether one or another of the known proofs is, in fact, Pascal's original one. This also applies to the simple proof given here.

Begin with the hexagon A_i, $i = 0, \dots, 5$ of Figure 1, and consider the circle through the points A_1, A_4 and P_1, where the first two points are (opposite) vertices, and the last is one of the "Pascal points" connected to them. This circle meets A_0A_1 and A_3A_4 at B_0 and B_1 respectively, and one uses arcs of the circles shown to find equal angles inscribed in them (or supplementary angles inscribed in opposite arcs). As a consequence, the triangles $P_1B_0B_1$ and $P_2A_0A_3$ have respectively parallel sides, that is, they are perspective from the point P_0. Therefore, P_0, P_1 and P_2 are collinear.

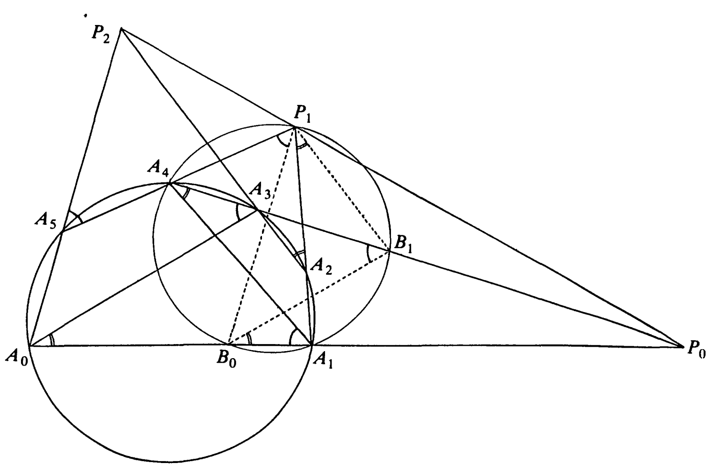


Figure 1

The proof also covers the case of $A_0A_1 \| A_3A_4$ (i.e., P_0 at infinity). Then, the triangles are translative, that is, P_1P_2 is parallel with A_0A_1 and A_3A_4. The only special case not covered by the proof concerns hexagons inscribed in a circle with parallels as opposite sides. This case, however, follows easily from appropriate arcs.

Whether Pascal gave this proof is open to debate, but it seems that this proof has not turned up for 350 years. On this point Professor Coxeter kindly has commented as follows: "It is indeed remarkable that this elegant proof was not

found in 350 years, and also somewhat remarkable that Guggenheimer came close to it in 1967 and then felt obliged to introduce a peculiar lemma." [3]

Anyway, the historic delay justifies some special attention for the heuristics of this simple proof.

The basic figure consists of two pencils of four lines joining points on a circle, viz. (Figure 2) A_0 and A_4 with, respectively, A_1, A_2, A_3 and A_5.

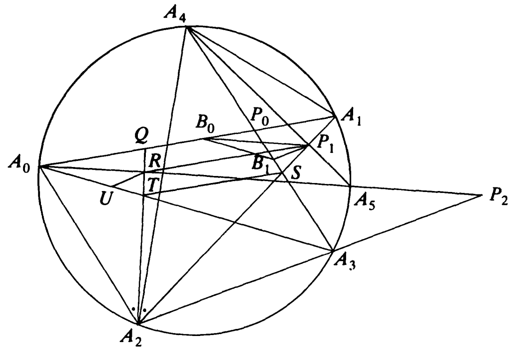


Figure 2

Evidently, the two pencils are congruent (equal angles between corresponding lines). Therefore, if $\triangle A_0A_2Q$ is made similar to $\triangle A_4A_2A_1$, the segments A_2Q and A_2A_1 are divided proportionally and $A_1A_0//P_1R//ST$. Now, the crucial idea is to build up this basic figure in a converse manner, starting with two given similar triangles: $\triangle A_0A_2Q \sim \triangle A_4A_2A_1$ and forgetting the circle.

Then, choose P_1 and R on, respectively, A_1A_2 and QA_2, such that $P_1R//A_1A_0$. Similarly S and T. Hereupon the following points are defined: $A_5 = A_4P_1 \cap A_0R$, $A_3 = A_4S \cap A_0T$, $P_0 = A_4S \cap A_0A_1$, $P_2 = A_0R \cap A_2A_3$.

To prove that P_0, P_1 and P_2 are collinear:

Consider $\triangle RA_0U$, $RU//P_2A_3$, and its translative image $\triangle P_1B_0B_1$. Then, B_0 lies on P_0A_0 as $P_0A_0//P_1R$, and B_1 lies on P_0A_3, because $P_1B_1 = RU = A_2A_3 \cdot RT/A_2T = A_2A_3 \cdot P_1S/A_2S$. Therefore, the triangles $P_1B_0B_1$ and $P_2A_0A_3$ are perspective from the point P_0 and, indeed, P_0, P_1 and P_2 are collinear.

Afterwards the crucial points B_0 and B_1 can be found directly. In fact, they lie on the circumcircle of $\triangle P_1A_1A_4$, because $\angle P_1B_0A_1 = \angle A_5A_0A_1 = \angle A_5A_4A_1 = \angle P_1A_4A_1$ and $\angle A_4B_1B_0 = \angle A_4A_3A_0 = \angle A_4A_1A_0 = \angle A_4A_1B_0$. Actually, drawing the circumcircle of $\triangle P_1A_1A_4$ is the very point of the new proof.

Background of the heuristics is the fact that the metric of the Euclidean plane can be defined by giving a pair of similar triangles. After that, all other metric properties must follow by means of parallels and proportionalities (affine tools).

REFERENCES

1. H. S. M. Coxeter and S. L. Greitzer, *Geometry Revisited*, New Mathematical Library, Random House and The L. W. Singer Company, 1967.
2. H. S. M. Coxeter, *The Real Projective Plane* (2nd ed.), Cambridge University Press, 1961.
3. H. W. Guggenheimer, *Plane Geometry and Its Groups*, Holden Day Inc., Cambridge, 1967.
4. R. A. Johnson, Advanced Euclidean Geometry, Dover Publications, New York, 1960.
5. N. A. Court, *College Geometry*, Barnes & Noble, New York, 1959.

Department of Mathematics
Technological University Eindhoven
The Netherlands, 5600 MB

NOTES

Edited by: **John Duncan**

The Mathematical Relationship Between Kepler's Laws and Newton's Laws

Andrew T. Hyman

1. INTRODUCTION. Whenever a new scientific theory comes down the pike, it is greeted by skeptics who demand proof that the new theory is as good as the theory it would displace. That is why "the major scientific problem of the [seventeenth] century" was to prove that Isaac Newton's law of gravity gives the same correct results as the older laws of Johannes Kepler [**4**]. This famous mathematical problem is solved below in an innovative way that requires no trigonometry, only elementary calculus, and none of the usual "clever tricks" [**8**].

Supposing that planets move according to Kepler's Laws (which are reviewed in Section 2 below), then it follows that planetary acceleration is given by Newton's central inverse-square equation (which is equation twelve below). This historic theorem was first proved by Newton, who thereby established his law of gravity as a respectable successor to Kepler's Laws. This same theorem is proved in Section 3, using simple and straightforward methods. The reverse theorem, according to which the central $1/R^2$ equation requires Keplerian orbits, is proved in Section 4.

The two theorems proved here were first published in Newton's 1687 *Philosophiae Naturalis Principia Mathematica*, or *Principia* for short. Newton admitted that the *Principia* is purposely "abstruse" ([**3**], p. 90), and a controversy persists as to whether Newton's proofs are entirely legitimate ([**2**], p. 30). Unlike the *Principia*, the brief proofs below are quite transparent.

Kepler's Laws are differentiated in Section 3 using only Cartesian coordinates, and this novel Cartesian approach contrasts with the usual technique of transforming to polar coordinates. Although the converse proof of Section 4 is fundamentally the same as those of a few other authors ([**5**], p. 178 of [**11**], and p. 625 of [**1**]), each step in Section 4 follows naturally and inexorably from what precedes it. No rabbits are pulled out of hats. The method of Section 4 is thus presented in a clear manner which compares favorably to the more common methods of solving the same problem, and also to various uncommon methods which are discussed in [**10**].

2. REVIEW OF KEPLER'S LAWS. Kepler deduced his laws from data supplied by the astronomer Tycho Brahe. Kepler's Laws are:

I. *Each planet moves along an ellipse with the Sun at a focus.*
II. *The line from a planet to the Sun sweeps out equal areas in equal times.*
III. *The square of a revolution's duration, divided by the cube of the orbit's greatest width, is the same for all planets.*

Kepler introduced the first two laws in his 1609 *Astronomia Nova*. The third or "harmonic" law was suggested in his 1619 *Harmonice Mundi*, and is often stated in terms of the length "a" of the semimajor axis ("a" is half the orbit's greatest width). The discovery of these laws marked the greatest advance since Aristarchus deduced nineteen centuries earlier that planets circle the Sun (see p. 2 of **[6]**).

Ellipses are, of course, the closed curves formed by intersecting a cone and a plane. They were studied by the ancient Greeks (see p. 119 of **[6]**) who proved that the distance to a point (the "focus") divided by the distance to a line (the "directrix") is a constant "eccentricity" ε. A beautiful proof of this focus-directrix property was devised in 1822 by G. P. Dandelin. Dandelin's proof appears at p. 546 of **[9]**, and it applies to both closed ($0 \leq \varepsilon < 1$) and open ($\varepsilon \geq 1$) conic sections.

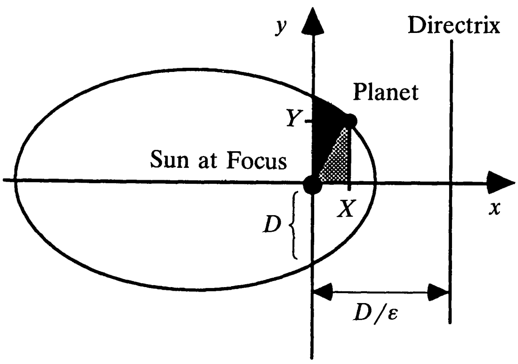


Figure 1

Kepler's Laws can be translated into equations by picturing a planet as a point-particle in the x-y plane, having coordinates (X, Y) at time t (see Figure). The Sun is located at the origin, and the planet's directrix is perpendicular to the x-axis at a distance D/ε from the Sun. "D" is called the "semi-latus-rectum" of the conic section. According to Kepler's First Law, the distance $R \equiv \sqrt{X^2 + Y^2}$ from the planet to the Sun is given by:

$$R = D - \varepsilon X. \tag{1}$$

Kepler's Second Law can be formulated in similarly simple terms. If the planet crosses the y-axis at time t_0, then the area swept between t_0 and t equals the area under the curve minus the triangular area beneath the line from Sun to planet. Hence, at all times,

$$\int_0^X y\,dx - XY/2 = C(t - t_0) \tag{2}$$

where "C" is the constant ratio of area swept to time elapsed (a new constant t_0 must be introduced whenever the planet crosses the x-axis).

The orbit's total area divided by a revolution's duration is clearly equal to C. Also, it is not difficult to prove that the area of an ellipse is πab with $a = D[1 - \varepsilon^2]^{-1}$ and $b = D[1 - \varepsilon^2]^{-1/2}$ (these two equations can be easily derived using equation one). Therefore, Kepler's Third Law is:

$$C^2/D = K \tag{3}$$

where the constant "K" is the same for all planets. In summary, Kepler's Laws are (1), (2), and (3).

3. PROOF OF CENTRAL $1/R^2$ EQUATION. Kepler's Laws will now be used to find the acceleration of a planet. Differentiating (1) produces:

$$\frac{1}{R}\left[X\frac{dX}{dt} + Y\frac{dY}{dt}\right] = -\varepsilon\frac{dX}{dt}. \tag{4}$$

Differentiating (2), using the Fundamental Theorem of Calculus, gives:

$$Y\frac{dX}{dt} - X\frac{dY}{dt} = 2C. \tag{5}$$

A bit of algebra applied to (4), (5), and (1) makes it clear that the two velocity components are:

$$\frac{dX}{dt} = \frac{2C}{D}\cdot\frac{Y}{R} \tag{6}$$

and

$$\frac{dY}{dt} = -\frac{2C}{D}\cdot\frac{X}{R} - \frac{2C\varepsilon}{D}. \tag{7}$$

Differentiating (5) yields:

$$Y\frac{d^2X}{dt^2} - X\frac{d^2Y}{dt^2} = 0. \tag{8}$$

Differentiation of the right-hand-side of (6) is facilitated by the following identity:

$$\frac{d}{dt}\left[\frac{Y}{R}\right] = \frac{X}{R^3}\cdot\left[X\frac{dY}{dt} - Y\frac{dX}{dt}\right]. \tag{9}$$

This identity is based solely upon the definition of R.† By differentiating (6) and plugging in (9), (5) and (3) one gets:

$$\frac{d^2X}{dt^2} = \frac{-4KX}{R^3}. \tag{10}$$

By (8) and (10),

$$\frac{d^2Y}{dt^2} = \frac{-4KY}{R^3}. \tag{11}$$

Equations (10) and (11) can be written compactly in terms of vectors.

$$\frac{d^2\vec{R}}{dt^2} = \frac{-4K\vec{R}}{R^3}. \tag{12}$$

Equation (12) is Newton's central inverse-square equation. This equation expresses Newton's law of gravity for the special case where planetary mass is negligible.

†Incidentally, note that $[X\dot{Y} - Y\dot{X}]$ is twice the areal speed (i.e., $R^2\dot{\theta}$ in polar coordinates), where dots denote differentiation. The referee has keenly observed that therefore equation (9) is basically $[\sin\theta]^{\cdot} = [\cos\theta]\dot{\theta}$.

4. RECOVERY OF KEPLER'S LAWS. It remains to be seen whether a bounded orbit could satisfy (12) if it is not Keplerian. In other words, could a planet be accelerating according to (12), and yet violate Kepler's Law? It will now be proved that such an orbit is impossible, by recovering Kepler's Laws from (12). By the way, it is taken for granted that motion is confined to a plane, though this assumption is easily justified ([**7**], p. 105).

Equations (10) and (11) lead to (8), and integrating (8) retrieves (5) and (2). Plugging (5) into the crucial identity (9) gives:

$$\frac{d}{dt}\left[\frac{Y}{R}\right] = \frac{-2CX}{R^3}. \tag{13}$$

On account of (13) and (10),

$$\frac{Y}{R} = \frac{C}{2K} \cdot \frac{dX}{dt} + A \tag{14}$$

where "A" is a constant of integration.

The identity (9) has been very useful here, and it would have been necessary to pull this identity out of thin air were it not for the context provided by Section 3. In this context, the identity (9) has arisen in a natural way (whereas other authors have indeed pulled this identity from out of the blue).

Interchanging "X" and "Y" in (9) produces another identity which together with (5) yields:

$$\frac{d}{dt}\left[\frac{X}{R}\right] = \frac{2CY}{R^3}. \tag{15}$$

So, by (11),

$$\frac{X}{R} = \frac{-C}{2K} \cdot \frac{dY}{dt} + B \tag{16}$$

where "B" is another constant. Plugging (14) and (16) into (5) yields:

$$\frac{C^2}{K} + AY + BX = R. \tag{17}$$

If $A = B = 0$, this describes a circle. If not, (17) represents a conic section with focus at the origin, eccentricity $[A^2 + B^2]^{1/2}$, and directrix given by:

$$\frac{C^2}{K} + Ay + Bx = 0. \tag{18}$$

This interpretation of (17) follows from a simple fact of analytic geometry: the distance from a point (x_0, y_0) to a line $ax + by + c = 0$ is equal to $|ax_0 + by_0 + c|[a^2 + b^2]^{-1/2}$. This well-known fact can also be applied to (18) in order to find the distance from focus to directrix, and it is thus evident that the focus-directrix distance is as described by (3). Consequently, if Newton's central inverse-square equation holds true then all bounded orbits must satisfy Kepler's Laws, which was to be demonstrated.

ACKNOWLEDGMENTS. I thank Dr. David Griffiths of Reed College for his help. I am also grateful to the referee for suggesting a number of improvements. Furthermore, I would like to express appreciation to the European Journal of Physics for printing an article similar to this one in July of 1993 (vol. 14, no. 4).

REFERENCES

1. R. Abraham and J. Marsden, *Foundations of Mechanics*, Benjamin, Reading, Massachusetts, Second Edition, 1978.
2. V. I. Arnol'd, *Huygens & Barrow, Newton & Hooke*, Birkhäuser, Basel, 1990.
3. G. Christianson, *In the Presence of the Creator*; *Isaac Newton and His Times*, Free Press, New York, 1984.
4. I. Cohen, essay in *Physics* by P. Tipler, Worth, New York, 1982, pp. 105–108.
5. H. Hart, Integration of the rectangular equations of motion in the case of a central force varying inversely as the square of the distance, *Messenger of Math.* 9 (1880) 131–132.
6. T. Heath, *A History of Greek Mathematics*, Vol. 2, Dover, New York, 1981.
7. W. Smart, *Textbook on Spherical Astronomy*, revised by R. Green, Cambridge Univ. Press, 1977. Smart's proof of planar orbits is in the same spirit as the proofs presented above. For instance, Smart does not use vector products.
8. B. Temple and C. Tracy, From Newton to Einstein, *Amer. Math. Monthly*, 99 (1992) 507–521.
9. G. Thomas and R. Finney, *Calculus and Analytic Geometry*, Addison-Wesley, Reading, Massachusetts, Sixth Edition, 1984.
10. R. Weinstock, Inverse-square orbits: Three little-known solutions and a novel integration technique, *Am. J. Phys.*, 60 (1992) 615–619.
11. A. Wintner, *The Analytical Foundations of Celestial Mechanics*, Princeton Univ. Press, 1941. I thank Dr. Robert Weinstock of Oberlin College for telling me of this book, and for his many helpful comments. Dr. Weinstock notes that Wintner's own references are incorrect (see ref. 20 of **[10]**).

Northwestern School of Law
Lewis and Clark College
Portland, Oregon 97219

A Short Proof of a Result on Polynomials

Răzvan Gelca

In this note we want to present a short proof of a result that appeared in **[1]**. For a polynomial $f(x) = \prod_1^n(x - x_i)$, with distinct real roots $x_1 < x_2 < \cdots < x_n$, we let $d = \delta(f) = \min_i(x_{i+1} - x_i)$ and $g(x) = f'(x)/f(x) = \sum_1^n 1/(x - x_i)$. If k is a real number then the roots of the polynomial $f' - kf$ are also real and distinct.

Proposition. *If for some j, y_0 and y_1 satisfy $y_0 < x_j < y_1 \le y_0 + d$ then y_0 and y_1 are not zeros of f and $g(y_0) < g(y_1)$.*

Proof: The hypothesis implies that for all i, $y_1 - y_0 \le d \le x_{i+1} - x_i$. Hence for $1 \le i \le j - 1$ we have $y_0 - x_i \ge y_1 - x_{i+1} > 0$ and so $1/(y_0 - x_i) \le 1/(y_1 - x_{i+1})$; similarly for $j \le i \le n - 1$ we have $y_1 - x_{i+1} \le y_0 - x_i < 0$ and again $1/(y_0 - x_i) \le 1/(y_1 - x_{i+1})$.

Finally $y_0 - x_n < 0 < y_1 - x_1$, so $1/(y_0 - x_n) < 0 < 1/(y_1 - x_1)$, and the result follows by addition of these inequalities.

Corollary. $\delta(f' - kf) > \delta(f)$.

Proof: If y_0 and y_1 are zeros of $f' - kf$ with $y_0 < y_1$ then they are separated by a zero of f and satisfy $g(y_0) = g(y_1) = k$. Hence from the proposition we can not have $y_1 \leq y_0 + d$, so $y_1 - y_0 > d$ as required.

REFERENCE

1. P. Walker, Separation of the zeros of polynomials, *Amer. Math. Monthly* (100)(1993) 272–273.

Department of Mathematics
The University of Iowa
Iowa City, IA 52242
rgelca@math.uiowa.edu

Institute of Mathematics
of the Romanian Academy
P.O. Box 1-764
70700 Bucharest Romania

Two Amusing Dynkin Diagram Graph Classifications

Robert A. Proctor

Here are a couple of simply stated graph classifications which can be used to amuse and amaze students and friends during tea or cocktail parties. It's fun to watch non-mathematicians theologically wrestle with the following notion: Mathematicians can *prove* that no one can come up with any solutions beyond the ones shown in the figures. Many people have been aware of the first classification for some time. The second one is an immediate consequence of a well known fact, but perhaps has not been formulated in this way before.

A *simple graph* is a graph which has no loops or multiple edges. I'll call it *labelled* if a positive real number has been assigned to each vertex.

Problem 1. *Find all connected labelled simple graphs whose labels satisfy the following condition: Twice any label is equal to the sum of the labels of the adjacent vertices.*

Answer. If you check this condition nine times, you can verify that the labels of the last graph in Figure 1 satisfy this requirement. For example, at the central vertex we have: $2 \times 6 = 4 + 5 + 3$. Surprisingly, up to an overall scalar multiple of the labels, *all* possible connected graphs labelled in this way are shown in Figure 1! There are two infinite families of solutions and then three specific peculiar "exceptional" solutions.

Problem 2. *Find all connected labelled simple graphs whose labels satisfy the following condition: Twice any label minus two is equal to the sum of the labels of the adjacent vertices.*

Answer. The *only* possibilities are shown in Figure 2. At the central vertex of the last graph we have $2 \times 270 - 2 = 182 + 220 + 136$. Again there are two infinite families of solutions followed by three exceptional solutions.

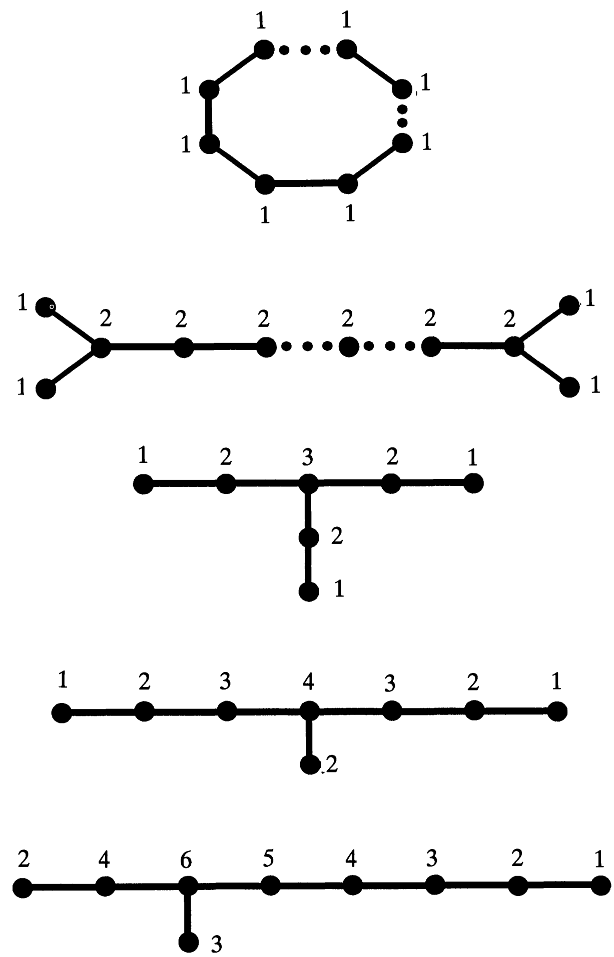
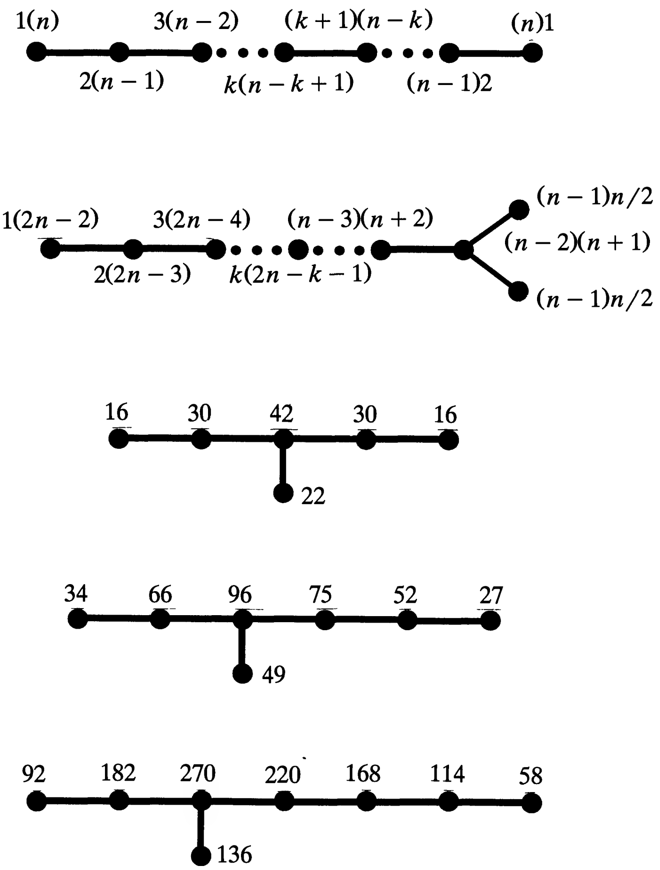


Figure 1

I've used Problem 1 to intrigue friends and students for years, but only recently did I notice Problem 2. I like it better than Problem 1 because the labels are much more entertaining, and because it's easier to explain the significance of its graphs to beginning graduate students: Without the labels, the graphs shown in FIGURE 1 are the extended Dynkin diagrams of types ADE, whereas the graphs of FIGURE 2 without their labels are just the ordinary Dynkin diagrams of types ADE. These play a role in the classification of simple Lie algebras (or groups), whereas the extended diagrams are used to help classify a more sophisticated family of objects, the affine Lie algebras. (Also, the solutions to Problem 2 are unique immediately, without the "overall scalar multiple" fine print needed with the solutions to Problem 1.)

There are many kinds of algebraic and geometric structures arising in mathematics which are "classified" by a list of some kind of Dynkin diagrams. For example, one could ask what are the possible finite subgroups of the orthogonal groups $O(n, \mathbb{R})$ which are generated by reflections. If we ignore the dihedral groups and require that the subgroup fix only the origin, then there is exactly one such subgroup for each member of the following list: $\mathsf{A}_n (n \geq 1)$, B_n $(n \geq 2)$, D_n



$n \geq 4$), E_6, E_7, E_8, F_4, G_2, I_3, and I_4. Here each X_n denotes a particular "Coxeter diagram" which has n nodes and which describes a particular subgroup of $O(n, \mathbb{R})$ up to conjugacy according to a certain recipe. These diagrams (shown on page 57 of [**BG**]) look similar to those appearing in our figures, but the edges are labelled and the vertices are unlabelled. For the details of this classification consult [**BG**], which was written for undergraduates. The names of our diagrams in FIGURE 1 are $\mathsf{A}_n^{(1)}$, $\mathsf{D}_n^{(1)}$, $\mathsf{E}_6^{(1)}$, $\mathsf{E}_7^{(1)}$, and $\mathsf{E}_8^{(1)}$ and in FIGURE 2 are A_n, D_n, E_6, E_7, and E_8. Although some aspects of the diagrams and the membership of the list can vary, it is usually readily apparent when a classification by Dynkin diagram-like objects is occurring. The diagrams of type E look quite distinctive, and it seems that one always has at least two diagrams of this type arising. The set of possible simple Lie algebras over $\mathbb{C}$ is indexed by the Dynkin diagrams A_n ($n \geq 1$), B_n ($n \geq 2$), C_n ($n \geq 3$), D_n ($n \geq 4$), E_6, E_7, E_8, F_4, and G_2. These diagrams (shown on page 58 of [**Hm1**]) are exactly what is meant by "Dynkin diagram." They are similar to Coxeter diagrams, except that some of the edges are directed. Usually the structures of the objects indexed by the version of Dynkin diagram at hand of type A, type D, or type E are easier to deal with than the structures of the objects indexed by the diagrams of other types. This fact is reflected at the diagram level by the diagrams of types ADE having all "easy" edges. The overall phenomenom of classification by Dynkin-like diagrams has many fascinating and mysterious aspects; consult [**HHSV**] for a survey.

Although the answers to Problems 1 and 2 are stated in terms of graphs, they are actually theorems in linear algebra! To see this, do the following: Let the variables $x_1, x_2, \ldots$ denote the as yet unknown vertex labels. In either problem, associate to each labelled graph with n vertices an $n \times n$ system of linear equations. For example, the first two requirements of Problem 2 corresponding to the first two vertices of the first graph in FIGURE 2 give rise to the equations $2x_1 - x_2 = 2$ and $-x_1 + 2x_2 - x_3 = 2$. For the graph of this form with 4 vertices, the system of equations giving all of the requirements for that graph is:

$$\begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 2 \\ 2 \end{bmatrix}.$$

In general, associate to any graph arising in either problem a matrix $A = (a_{ij})$ of the following form: The main diagonal entries $a_{ii} = +2$; the off-diagonal entries a_{ij} are -1 if vertex i is connected to vertex j and 0 otherwise. Conversely, given any $n \times n$ matrix A with $a_{ii} = +2$ and $a_{ij} = a_{ji} = -1$ for some pairs (i, j) and $a_{ij} = 0$ otherwise, one could depict it with a simple graph wherein vertex i is connected to vertex j whenever $a_{ij} = -1$. We say that such a matrix A is *connected* if its corresponding graph is connected. Define three column vectors of length n as follows: $v := (x_1, x_2, \ldots, x_n)^{\mathsf{T}}$, $0 := (0, 0, \ldots, 0)^{\mathsf{T}}$, and $2 := (2, 2, \ldots, 2)^{\mathsf{T}}$. Let's say that v is *positive* if $x_i > 0$ for $1 \le i \le n$.

So Problem 1 (respectively Problem 2) actually is asking us to find all connected matrices A of this form for which the linear system $Av = 0$ (respectively $Av = 2$) has a positive solution. With these formulations the answers stated at the beginning of this note are mostly derived on pages 47–54 of **[Kac]**. These eight pages can be read and understood by themselves, provided that you have had a good course in linear algebra. Kac is interested in such questions because the matrices A, known as generalized Cartan matrices in Lie theory, describe the structure of certain kinds of Lie algebras. On these pages he uses basic linear algebra techniques to investigate the existence of positive solutions v to systems of linear inequalities such as $Av > 0$ and $Av \ge 0$, assuming that A has a certain form. The notions of positive definiteness and positive semi-definiteness play a key role.

Here are the details. Part (e) of Proposition 4.7 and parts (b) and (c) of Theorem 4.8 of **[Kac]** give the answer to Problem 1. For Problem 2 start with Theorem 4.3. By this result, since A cannot be of type (Aff) or (Ind), it must be of type (Fin). Then part (a) of Theorem 4.8 tells us that the graph S must be one of the graphs listed in FIGURE 2. My contribution is to supply the particular right hand side $(2, 2, \ldots, 2)^{\mathsf{T}}$, thereby forming Problem 2 as stated above. It is easy to check that each of the labellings given in FIGURE 2 meet the requirements. In each case only one such labelling is possible, since Theorem 4.3 of **[Kac]** tells us that $\det A \neq 0$ whenever A is of type (Fin).

The operator that doubles a vertex label and then subtracts the adjacent labels may be thought of as a discrete version of $-\Delta$, where Δ is the Laplace operator.

Now a few comments for people who are familiar with simple Lie algebras. The matrices A associated to each of the graphs of FIGURE 2 are just the Cartan matrices for the root system **[Hm1]** associated to the graph. Multiplying a column vector from the left by A has the following interpretation: You are just converting a column vector of coordinates with respect to the simple root basis to the fundamental weight basis. Since the coordinates of the famous vector $\rho = \delta$ are

$(1, 1, \ldots, 1)^T$ with respect to the fundamental weight basis, the labels appearing on the vertices are just the coordinates of the vector 2ρ in the simple root basis. As such, they appear in tables such as those at the end of **[Bou]**. The extended Dynkin diagrams of FIGURE 1 can be understood in the context of ordinary root systems as follows. If you adjoin a vertex to the Dynkin diagram of a root system which represents the lowest root $-\beta$ as described on page 95 of **[Hm2]**, then in the ADE cases the diagrams of FIGURE 1 will result. The labels on the remaining vertices give the expansion of β with respect to those simple roots.

Why was I thinking about this recently? In 1980 the labels of FIGURE 2 arose in my thesis (which was written under the direction of Richard Stanley). A member of my committee, George Lusztig, asked me if I knew of an existing interpretation of these mysterious positive integers. Last year while flipping through the recent **[MPR]**, the numbers jumped out at me twelve years late: The typography of the tables in **[Bou]** was such that I hadn't noticed them before. Fortunately, I was passed on my defense nonetheless! (The paper version of that chapter of my thesis **[Pro]** describes a Dynkin diagram classification of order diagrams of finite partially ordered sets. That result has a very similar flavor to the subject matter of this note.)

REFERENCES

[BG] L. Grove, C. Benson, *Finite Reflection Groups*, 2nd ed., Springer-Verlag, New York, 1985.

[Bou] N. Bourbaki, *Groupes et Algebres de Lie*, Chapitres 4, 5, et 6, Hermann, Paris, 1968.

[HHSV] M. Hazewinkel, W. Hesselink, D. Siersma, F. Veldkamp, The ubiquity of Coxeter-Dynkin diagrams, Nieuw Arch. Wisk. (8) 25 (1977), 257–307.

[Hm1] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, New York, 1972.

[Hm2] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press, Cambridge, 1990.

[Kac] V. Kac, *Infinite Dimensional Lie Algebras*, 3rd ed., Cambridge University Press, Cambridge, 1990.

[MPR] W. G. McKay, J. Patera, D. W. Rand, *Tables of Representations of Simple Lie Algebras Vol. I*, Les Publications CRM, Montreal, 1990.

[Pro] R. Proctor, A Dynkin diagram classification theorem arising from a combinatorial problem, Advances in Math. 62 (1986), 103–117.

Department of Mathematics
University of North Carolina
Chapel Hill, NC 27599

Professor Wedderburn's request that the Association be represented on the Editorial Staff of the Annals of Mathematics by two associate editors was favorably considered. The Trustees authorized President Ford to appoint a committee of three, including himself, with power to select and nominate two associate editors of the Annals of Mathematics. President Ford appointed Professors Cairns and Slaught as the other members of this committee. It was understood that the Annals volume will be still further enlarged and it was felt that our subvention to the Annals is now inadequate. The Trustees, therefore, voted to increase the annual subvention to $300.

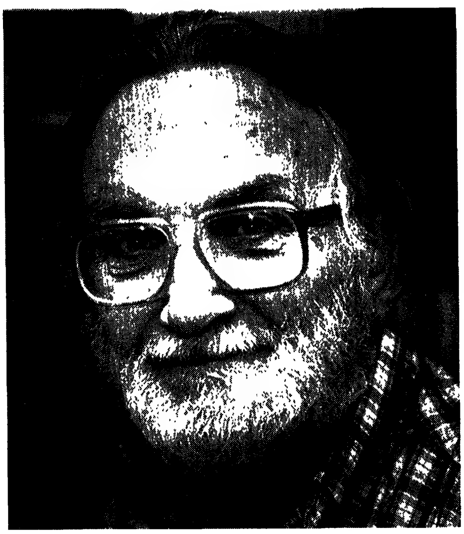
American Mathematical Monthly
34, (1927) p. 117

Postcards from Max

As remembered by Paul Halmos

Editor's note: *Max Zorn died on March* 9, 1993.

Max Zorn was born twenty nine years before Zorn's Lemma, and Zorn's Lemma, the technique and the attitude, will go on living for centuries. For Max the lemma was a remark—the title of his paper on the subject is "A remark on method in transfinite algebra"; it was John Tukey who baptized the result.



Max was a friend of mine, a good friend. We became acquainted in 1969, when I gave a colloquium talk at Bloomington. Max came to the tea before the talk—he came to tea every day, whether there was a colloquium or not—and, in accordance with his custom, he came prepared. On a wrinkled slip of paper (it might actually have been the back of a used envelope) he had scribbled the questions he wanted me to answer—what is my opinion on the work of so-and-so?, how is this work connected with something I wrote ten years before?, has there been any recent progress along the lines of such-and-such? I don't remember any colloquium at which he didn't ask a question afterward (and sometimes during)—a relevant question, a pertinent question, a sharp question. His questions showed that he understood the subject, understood the talk, and was ready to understand and remember the answers. His questions were not intended to be embarrassing, but if the speaker was not thoroughly checked out on all aspects of the subject of his own talk, they could become embarrassing. Max didn't mean to cause pain, and he cheerfully indicated a friendly acceptance of even a vague answer.

Does everybody remember the Piccayune Sentinel? Yes, I spelled it right—the misspelling is Max's own and I faithfully copied both c's. I don't know just when he started it; the first issue that I have a copy of is dated November 1950. It was a one-sheet affair that Max called the world's smallest newspaper and that he gave to a few friends (usually by putting copies into his colleagues' mailboxes, and rarely, for distant friends, by mailing them). One issue I have is labelled "partially late". The contents of the Piccayune Sentinel were of the same kind as Max himself and his postcards (and as unpredictable and as confusion-inducing)—just longer and more widely distributed.

We were colleagues at Indiana for many years, and we had a routine: most afternoons we would troop over to the physicists' common room in Swain West (the mathematicians couldn't afford such a large and elegant place), get our coffee and cookies, and sit gossiping on the couch by the permanently curtained windows (heaven forbid that some unwanted light or air should enter). Our gossip was never malicious (well, hardly ever): it was about people in the profession (who is moving where and how much will he get paid?), about the profession (could square-summable power series really be relevant to the Riemann hypothesis?), about local matters (who will teach what when and will that room be big enough to hold the class?)—and about books, about movies, about travel, about languages, about anything that had a momentary or a permanent interest for at least one of us. We never ran out of subjects; I looked forward to our meetings, and when some catastrophe prevented one, I missed it.

One conversation we had bothered me afterward, and I was moved to write down my concern in a letter to Max. The letter didn't go through the U.S. Mail—I just put it into Max's box. Here is what I wrote.

"Something you said yesterday worries me—I kept thinking about it during the night and it kept worrying me. You said that you had bad judgement and that you were a failure—two statements with which I thoroughly disagree.

"Of all people I know you are the one who has the sharpest, finest, clearest insight into all of mathematics, and, for that matter, into most of human life. Your tastes and mine (in mathematics, and sometimes in other things) are not always the same—but your insight and your judgement are impressive.

As for failure: that's nonsense. You are respected by everyone who knows you (and by thousands of others), and you are liked by everyone who knows you or ever came anywhere near you. You are a mathematician. Most people no longer know whether your work was algebra, or complex functions, or something funny about semigroups, or whatever—but they respect you for your reputation, for (if you'll pardon the expression) your lemma, for your questions, for your wit (a non-accidental cognate of Wissenschaft), for your understanding. You have written, you have taught, you have inspired—is that a failure? I wish I were one!"

Max answered me with a hand-written note that I found in my box the next day.

"In school I heard:

Eigenlob stinkt,
Freundeslob hinkt,
Feindeslob klingt.
(But) thanks."

I wasn't quite sure of all the verbs, so I checked them in a dictionary; roughly (not too roughly) they mean stinks, limps, and rings (respectively).

I left Indiana twice—meaning that I accepted an invitation from another university, moved, returned after a couple of years, and some years later moved again—and we started corresponding. The first time, when at tea one day I said "Max, I'll be leaving", he said "For bad?". That, by the way, is typical of his use of language—he knew idiomatic English perfectly, and had enough control over it that he could twist it to communicate delicate shades of meaning elegantly and efficiently.

He was an unpredictable correspondent. I am a garrulous one—I tend to write repetitive letters full of many details that probably no one besides me is interested in—and he varied from stories with smiles in them to almost brusquely short hello-good-byes. As the years went on, I got in the habit of writing him a longer letter (three or four single-spaced pages) approximately once a month, and he got

in the habit of a short and mysterious friendly postcard approximately twice a year. The operative word is mysterious: he used abbreviations that he invented as he was writing, and with them he referred to happenings, past and future, that I had no way of knowing anything about. Every now and then I really wanted to understand the latest mystery and I demanded an explanation (in my next letter, or even by telephone)—and he was always goodnatured about it, and while seemingly puzzled that someone could fail to understand something that clear, he cheerfully explained. The result was sometimes understandable.

The first Zorn letter that I saved was one of the long friendly kind, two hand-written pages, and it is signed: "as never before, Max". A few years later another letter ends with: "as before, Max". One postcard consisted of the following sentence: "If $f(x, y)$ is such that $f(1, y), f(2, y), \ldots, f(n, y), \ldots$ are computable, then I want $f(x, y)$ to be computable". A couple of years later (again a postcard): "$\exists$ I (Nach Kant ist die Existenz des eigenen Ich nicht trivial.)" Still another: "Is the symbol of the symbol (defined and) the same as the symbol?" Again: "Is a random variable a function or an equivalence class of functions?" And: "Sum, ergo dubito." One letter I received from Max was one typewritten page, on the back of which appeared a backward carbon copy of the same letter, and a handwritten footnote: "You can see that I tried to keep a copy. Long live Freud!"

The letters and postcards came oftener at the beginning than later on—perhaps six to eight times a year—toward the end I was lucky if I got two a year. His last letter came in December 1992; it ends with "I plead fatigue, Max."

I miss Max.

UNSOLVED PROBLEMS

Edited by: **Richard Guy**

In this department the MONTHLY presents easily stated unsolved problems dealing with notions ordinarily encountered in undergraduate mathematics. Each problem should be accompanied by relevant references (if any are known to the author) and by a brief description of known partial or related results. Typescripts should be sent to Richard Guy, Department of Mathematics & Statistics, The University of Calgary, Alberta, Canada T2N 1N4.

A Quarter Century of *Monthly* Unsolved Problems, 1969–1993

Richard K. Guy

A most valuable and timely contribution by Stanley Rabinowitz, which will hopefully greatly reduce the amount of duplication and rediscovery that presently occurs, and will be a boon to all editors of problems sections of all kinds, is his series

Index to Mathematical Problems

of which Volume 1, 1980–1984, is available. It is obtainable from MathPro Press, Westford MA.

References in brackets are to year and page numbers of this MONTHLY, while dates in parentheses refer to publications listed at the end, and other items are labelled (tbp) if they are likely to be published formally, or as written communications (wrc) if publication plans are not presently known. Dates and pages in brackets are also appended to items in the bibliography indicating where the problem originally appeared in the MONTHLY.

In [1969, 54] Victor Klee launched this section of the MONTHLY with the notorious equichordal problem, which goes back to World War I. It gets a mention in reviews by both DeTurck (1993) and Falconer (1993), but even as they wrote the problem was finally being solved by Marek Rychlik (tbp).

The graceful graph [1969, 1128] bibliography is now best regarded as the purview of Joseph Gallian, to whom items should be sent. My somewhat out-of-date version contains 232 papers by 410 authors, only 169 distinct.

Klee [1970, 63] asked for the maximum length of a d-dimensional snake, where by **snake** is meant a simple circuit in the d-cube which has no chords. If we denote this maximum length (number of edges) by $s(d)$, then Abbott and Katchalski (1991) show that $s(d) \geq 77 \times 2^{d-8}$. Their paper contains a very good bibliography.

Erdős and Guy [1973, 52] raised several questions concerning the crossing numbers of graphs; Sýkora and Vrťo (1992) give the following lower bounds for the crossing number of the complete bipartite graph, the edge-skeleton of the n-

dimensional cube, and the complete graph, on an orientable surface of genus g.

$$\nu_g(K_{m,n}) > \frac{m^2n^2}{1200g} - \frac{mn(m+n)}{2} \qquad \nu_g(Q_n) > \frac{4^n}{1500g} - n^2 2^{n-1}$$

$$\nu_g(K_n) > \frac{n^4}{6075g} - \frac{n^3}{2}$$

Steven Finch extended Queneau's computations of "Ulam sequences" [1973, 919; 1975, 998; 1987, 962], a (u, v)-**sequence** of positive integers $\{a_i\}$ being defined by $a_1 = u$, $a_2 = v$ and, for $n > 2$, a_n is the least integer expressible *uniquely* as the sum of two distinct earlier members. Queneau showed that the (2,5)-, (2,7)- and (2,9)-sequences are **regular** in the sense that their differences are ultimately periodic. Finch (1991, 1992) proved that if the (u, v)-sequence has only finitely many even terms, then it is regular. Schmerl and Spiegel (tbp) prove that the $(2, v)$-sequence has just two even terms for any odd $v > 3$.

Leech [1975, 923] asked, for each integer n, what is the greatest integer N such that there exists a tree with n nodes, and edges labelled with integers, in which the distances between pairs of nodes include the consecutive values $1, 2, \ldots, N$? Here the distance is the sum of the labels on the unique path joining the nodes. Work of Gibbs and Slater (1991), Herbert Taylor (1991) and Yang Yuan-Sheng (wrc) has improved the results for paths and for more general trees to

n	2	3	4	5	6	7	8	9	10	11	12
paths	1	3	6	9	13	18	24	29	37	45	(51)
trees	1	3	6	9	15	20	26	34	41	(48)	(55)

where the entries in parentheses are not necessarily best possible.

Joseph Gerver (tbp) and evidently Ben Logan before him in 1976, probably found the maximum area sofa that you can move round a corner [1976, 188 and see 1977, 811 and 1991, 974]. A partial description of it is given by Ian Stewart (1992). Its boundary comprises three straight line segments, four arcs of radius $\frac{1}{2}$, seven arcs of involutes of a circle, and four arcs of involutes of involutes of a circle. Its area is ≈ 2.2195.

In [1983, 35] I warned readers not to try to solve various problems, one of which was the notorious $3x + 1$ problem. Two years later [1985, 3] Lagarias gave a valuable survey and bibliography. Recently he and Weiss (1992) have given two interesting stochastic models for the problem which independently produce the same constant $\gamma_0 \approx 41.677647$ for $\limsup_{n\to\infty}(\sigma_\infty(n)/\ln n)$, where $\sigma_\infty(n)$ is the number of iterations of the famous function $T(n) = n/2$ (n even), $T(n) = (3n + 1)/2$ (n odd) required to get to the value 1.

In [1991, 974–975] we compared the problem of Forcade, Lamoreaux and Pollington [1986, 119; 1989, 905] with the special case asked by Basil Gordon. The papers of Chandler (1988) and of Forcade and Pollington (1990) are relevant. Blair Kelly III has done a computer search, revealing that $n = 85$ is the smallest counterexample. The next counterexamples are for $92 \le n \le 108$, $n = 112$, $n = 113$, $115 \le n \le 118$ and $121 \le n \le 156$. He says that it is natural to conjecture that there are no Gordon maps for $n > 120$.

Tomaszewski [1986, 280] considered n real numbers $a_1, \ldots, a_n$ satisfying $\Sigma_{i=1}^n a_i^2 = 1$ and asked if, of the 2^n sums of the form $\Sigma \pm a_i$, it is possible that there are more with $|\Sigma \pm a_i| > 1$ than there are with $|\Sigma \pm a_i| \le 1$. Holzman and Kleitman (tbp) establish the sharp lower bound $3/8$ for the case where the inequality is strict, $|\Sigma \pm a_i| < 1$, but for the original problem the gap between $3/8$ and the conjectured $1/2$ is still open.

Terry Raines (wrc) says that Erdős, and not your editor, was right: Pambuccian [1986, 627] asked for $a(n)$, the smallest integer a for which there's an integer b, $0 < b < a$, $a \perp b$, such that $a + b, 2a + b, \ldots, na + b$ are all composite and asked if $a(n)$ was always prime. Raines notes that for $n = 135$, $a(n) = 8207 = 29 \cdot 283$, with $b = 3251$. He has carried his computations to $n = 180$, and each of $150 \le n \le 173$ provide further counterexamples.

In [1988, 927] Tony Gardiner showed that the following four questions are equivalent: for which primes p, if any, (A) is $\binom{2p}{p} \equiv 2 \bmod p^4$? (B) is $\sum_1^{p-1} r^{-1} \equiv 0 \bmod p^3$? (C) is $\sum_1^{p-1} r^{-2} \equiv 0 \bmod p^2$? (D) does p divide the numerator of the Bernoulli number B_{p-3}? Scott Hochwald (tbp) notes that the questions are indeed equivalent, but that Gardiner's final congruence is incorrect and should be replaced by the statement that

$$S_{p-3}(p) + \frac{p-3}{2}[(p-1)!]^2\left(1 + \frac{1}{2^2} + \cdots \frac{1}{(p-1)^2}\right)$$

is divisible by p^2. The only known prime was 16843, but on a recent visit to Calgary Richard Macintosh found á second example, 2124679.

In [1989, 31] R. J. McG. Dawson asked if there was a subset of a square that contains disjoint connected sets A and B each containing two opposite corners, but does not contain two disjoint connected sets each containing two adjacent corners. Keith Whittington (1991) provides the counterintuitive affirmative answer.

In [1989, 129] Clark Carroll asked for polynomials with integer roots whose derivatives all have integer roots. For cubics the answer is known and can be found, for example, in Walter (1987) or in Buddenhagen, Ford and May (1992); see also MONTHLY problem E3221, solved in [1989, 841–842]. For quartics, there are unpublished papers of Zagier (wrc), Buddenhagen and Ford (wrc) and the present writer, who may have been misleading in [1989, 907–908]. The situation is that for quartics with a repeated root there is an infinity of solutions, given essentially by the rational points on the elliptic curve $y^2 = x^3 - 156x + 560$, **576I2** in Cremona (1992). It seems unlikely that there are quartics with all roots distinct, nor higher degree polynomials unless they have sufficiently many repeated roots, but these may still be open questions.

In connexion with Sands's guessing game [1990, 314], see Joel Spencer's (1992) paper.

I apologize that what were offered as unsolved problems in [1992, 74] are in fact well known results. Many of the big names in combinatorial number theory are among those who have written to say that Matiyasevich's generalized harmonic numbers are essentially Stirling numbers of the first kind, and that his conjectures follow fairly easily from known properties. See especially Glaisher (1900), but also Nielsen (1906), Carlitz (1953), Olsen (1966) and Comtet (1974).

In [1992, 178] John Connett asked if a bottle with an inside perfectly reflecting surface could be designed so that a beam of light shone into it was permanently trapped. Robert Dawson, Jan Mycielski and Lior Pachter immediately and independently designed such bottles; their results have been combined (1993). Other solutions were received from M. E. Taylor (wrc), from Madhu Vairy Nayakkankuppam (wrc) and from the PCC Rock Creek Math Club—see Bercowitz et al. (wrc).

The page numbers for Connett's second reference should be 1113–1122.

In connexion with the Gordon game [1992, 567] Bob Kibler writes: For the fourteen groups of order 16, White wins only in the cyclic case (by playing to 8). In D_5 White wins by playing to an element of order 5. In D_7 by playing to an element

of order 2. In Z_{12} and Z_{14} by playing to the element of order 2. Black wins in Z_{15}, Z_{17}, D_6 and $Z_2 \times Z_2 \times Z_3$. In Z_{18} White wins by playing to 6—does he also win by playing to 9?

Fatin Sezgin (wrc) applied various tests to the Mycielski sequence [1992, 373] as a result of which he asserts that it cannot be considered as random.

Neil Calkin notes the relevance of Peter Cameron's survey article (1987) and his own thesis (1988) to Steven Finch's 0-additive sequences problem [1992, 671]. Finch has calculated $1\frac{1}{2}$ million terms of the sequence $\{a_n\}$, where $\{a_1, \dots, a_6\} = \{3, 4, 6, 9, 10, 17\}$ and for $n \geq 6$, a_{n+1} is the least integer greater than a_n which is *not* of the form $a_i + a_j$, $i < j$; without detecting any regularity (ultimate periodicity of the differences). Finch believes that this may be due to a massive initial segment of irregular values, while Calkin suspects that there may be counterexamples to Finch's conjecture. They are preparing a joint paper.

David Callan (wrc) solved Parker's permutation problem [1993, 287] affirmatively, and gave an alternative proof that it involves the Catalan numbers. Volker Strehl notes that the problem is not new, and has been solved both qualitatively and quantitatively. It appears, in the 'Griggs' version of the last three lines of [1993, 289], in various contexts: completion of latin squares, a bus scheduling problem, number of terms in the permanent of a circulant matrix. Marshall Hall (1952) attributes the problem to George Cramer, and generalizes and solves it for general finite abelian groups. Marica and Schönheim (1969) apply the result to latin square completion. Brualdi and Newman (1970) solve the enumeration problem by a method closely paralleling that of Gessel in the article under discussion. Chang (1979) uses Hall's theorem and cites Marica and Schönheim. Salzborn and Szekeres (1979) prove Hall's theorem but give no references to earlier work; their motivation was a bus scheduling problem.

REFERENCES

Harvey L. Abbott and M. Katchalski, On the construction of snake in the box codes. *Utilitas Math.*, 40 (1991) 97–116. [1970, 63]

S. Berkowitz, S. Dahlstrom, G. Madrid, M. McKelvey and F. W. Simmons, Solution to Connett's light-trapping problem (preprint). [1992, 178]

R. A. Brualdi and M. Newman, An enumeration problem for a congruence equation, *J. Res. Nat. Bur. Stand.*, 74B (1970) 37–40; *MR* 42 #1753. [1993, 287]

Jim Buddenhagen, Charles Ford and Mike May, Nice cubic polynomials, Pythagorean triples and the law of cosines, *Math. Mag.* 65 (1992) 244–249. [1989, 129]

Jim Buddenhagen and Charles Ford (wrc), Nice polynomials (1992 preprint). [1989, 129]

David Callan, Parker's conjecture is true! (preprint, April, 1993) [1993, 287]

Neil J. Calkin, Sum-free sets and measure spaces, PhD thesis, Univ. of Waterloo, 1988. [1992, 671]

Neil J. Calkin and Steven R. Finch, Necessary and sufficient conditions for a sum-free set to be ultimately periodic. [1992, 671]

Peter J. Cameron, Portrait of a typical sum-free set, Surveys in Combinatorics 1987, *London Math. Soc. Lecture Notes*, 123 (1987) Cambridge Univ. Press, 13–42. [1992, 671]

Leonard Carlitz, Note on a theorem of Glaisher, *J. London Math. Soc.*, 28 (1953) 245–246; *MR* 14 726b; rNT B72-12. [1992, 74]

Leonard Carlitz, A Theorem of Glaisher, *Canad. J. Math.*, 5 (1953) 306–316; *MR* 14 1064b; rNT B72-15. [1992, 74]

K. A. Chandler, Groups formed by redefining multiplication, *Canad. Math. Bull.*, 31 (1988) 419–423; *MR* 89m: 20021. [1986, 119]

Gerard J. Chang, Complete diagonals of latin squares, *Canad. Math. Bull.*, 22 (1979) 477–481; *MR* 81g:05033. [1993, 287]

Louis Comtet, Advanced Combinatorics, Reidel, Dordrecht, 1974, p. 229. [1992, 74]

John E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

Dennis DeTurck, Review of *Unsolved Problems in Geometry*, *Math. Intelligencer*, 15 (1993) 71–72. [1969, 54]
Kenneth Falconer, Review of *Old and New Unsolved Problems in Plane Geometry and Number Theory*, *Math. Intelligencer*, 15 (1993) 72–74. [1969, 54]
S. Finch, Conjectures about s-additive sequences, *Fibonacci Quart.*, 29 (1991) 209–214. [1973, 919]
S. Finch, On the regularity of certain 1-additive sequences, *J. Combin. Theory Ser. A*, 60 (1992) 123–130. [1973, 919]
S. Finch, Patterns in 1-additive sequences, *Experimental Math.*, 1 (1992) 57–63. [1973, 919]
R. W. Forcade and A. D. Pollington, What is special about 195? Groups, nth power maps and a problem of Graham, in R. A. Mollin (editor) Number Theory, *Proc. 1st Conf. Canad. Number Theory Assoc., Banff, 1988*, de Gruyter, 1990, 147–155. [1986, 119]
Joseph L. Gerver, On moving a sofa around a corner, *Geom. Dedicata*, 42 (1992) 267–283; *MR* 93d:51040. [1976, 188]
Richard A. Gibbs and Peter J. Slater, Distinct distance sets in a graph, *Discrete Math.*, 93 (1991) 155–165. [1975, 923]
J. W. L. Glaisher, Congruences relating to the sums of products of the first n numbers and to other sums of products, *Quart. J. Pure Appl. Math.*, 31 (1900) 1–35. [1992, 74]
Marshall Hall, A combinatorial problem on abelian groups, *Proc. Amer. Math. Soc.*, 3 (1952) 584–587; *MR* 14, 350b. [1993, 287]
Scott H. Hochwald (tbp), How I rediscovered Kummer's congruence. [1988, 926]
Ron Holzman and Daniel J. Kleitman, On the product of sign vectors and unit vectors, *Combinatorica*, (to appear). [1986, 280]
J. C. Lagarias and A. Weiss, The $3x + 1$ problem: two stochastic models, *Ann. Appl. Probab.*, 2 (1992) 229–261. [1983, 35]
J. Marica and J. Schönheim, Incomplete diagonals of latin squares, *Canad. Math. Bull.*, 12 (1969) 235; *MR* 40 #55. [1993, 287]
N. Nielsen, Handbuch der Theorie der Gammafunktion, 1906; Chelsea, 1966. [1992, 74]
F. R. Olsen, An extension of a theorem of Nielsen, *Portugal. Math.*, 25 (1966) 63–66; *MR* 35 #4190; rNT B72-28. [1992, 74]
Marek Rychlik, A complete solution of the equichordal point problem of Fujuwara, Blaschke, Rothe and Weizenböck, *Inventiones Math.*, (1993). [1969, 54]
Franz J. M. Salzborn and G. Szekeres, A problem in combinatorial group theory, *Ars Combin.*, 7 (1979) 3–5; *MR* 81b:05021. [1993, 287]
James Schmerl and Eugene Spiegel (tbp), The regularity of some 1-additive sequences, *J. Combin. Theory Ser. A*. [1973, 919]
Fatin Sezgin, On the Mycielski sequence (preprint) Oct 1992. [1992, 373]
F. Shahrokhi, O. Sýkora, L. A. Székely and I. Vrťo, Lower bounds for the crossing number of a graph drawn on a compact 2-manifold, *Proc. 7th Internat. Conf. Graph Theory, Combin., Algorithms, Appl.* (1992). [1973, 52]
Joel Spencer, Ulam's searching game with a fixed number of lies, *Theor. Comput. Sci.*, 95 (1992) 307–321. [1990, 314]
Ian Stewart, Sofa, so good, Chapter 16 of *Another Fine Math You've Got Me Into ...*, W. H. Freeman, 1992. [1976, 188]
O. Sýkora and I. Vrťo, Edge separators for graphs of bounded genus with applications, *Proc. 17th Internat. Workshop Graph Theoretic Concepts Comput. Sci.*, 1991, Springer Lecture Notes in Comput. Sci., 570 (1992) 159–168. [1973, 52]
Herbert Taylor, A distinct distance set of 9 nodes in a tree of diameter 36, *Discrete Math.*, 93 (1991) 167–168. [1975, 923]
M. E. Taylor, Ray trapping obstacles in the plane (preprint). [1992, 178]
Johann Walter, Über ganze rationale Funktionen dritten Grades mit ganzzahligen Koeffizienten, bei denen Nullstellen und Extrema zugleich ganzzahlig sind, *Praxis Math.*, 29 (1987) 489–492. [1989, 127]
Keith Whittington, Cross the square, this MONTHLY, 98 (1991) 833–834. [1989, 31]
Don Zagier (wrc), Quartic polynomials all of whose derivatives have integer roots (1989 preprint). [1989, 127]

Department of Mathematics
University of Calgary
Calgary, Alberta
CANADA T2N 1N4

PROBLEMS AND SOLUTIONS

Edited by:
Richard T. Bumby, Fred Kochman and Douglas B. West

Proposed problems should be sent to the MONTHLY PROBLEMS address given on the inside front cover. Please include solutions, relevant references, etc. Three copies are requested.

Solutions of published problems should arrive before May 31, 1994 at the MONTHLY PROBLEMS address given on the inside front cover. Solutions should be typed with double spacing, including the problem number and the solver's name and mailing address. Two copies suffice. A self-addressed postcard or label should be included if an acknowledgment is desired.

*An asterisk (*) after the number of a problem, or part of a problem, indicates that no solution is currently available. Partial solutions will be useful in such cases. Otherwise, the published solution is likely to be based on a solution which is complete and correct. Of course, an elegant partial solution or a method leading to a more general result is always useful and welcome. In addition, references to other appearances of MONTHLY problems or to solutions of these problems in the literature are also solicited.*

PROBLEMS

10346. *Proposed by David Doster, Choate Rosemary Hall, Wallingford, CT.*

Prove that, for all primes p,

$$\sum_{k=1}^{p-1}\left\lfloor\frac{k^3}{p}\right\rfloor = \frac{(p-2)(p-1)(p+1)}{4}; \qquad (A)$$

and

$$\sum_{k=1}^{M}\left\lfloor\sqrt[3]{kp}\right\rfloor = \frac{(3p-5)(p-2)(p-1)}{4}, \qquad (B)$$

where $M = (p-1)(p-2)$.

10347. *Proposed by T. S. Nanjundiah, University of Mysore, Mysore, India.*

For integer $n \geq 1$, define real numbers R_n by

$$R_1 = 1 \qquad R_{k+1} = 1 + \frac{k}{R_k} \quad (k \geq 1).$$

Prove that

$$\sqrt{n-\tfrac{3}{4}}+\tfrac{1}{2}\le R_n\le\sqrt{n+\tfrac{1}{4}}+\tfrac{1}{2}$$

for $n \geq 1$.

10348. *Proposed by Jiang Huanxin, student, FuDan University, ShangHai, China.*

Let D, E, F be distinct points on the sides BC, CA, and AB respectively of $\triangle ABC$. Let $\alpha = \angle BDF$, $\beta = \angle FDA$, $\gamma = \angle ADE$, and $\delta = \angle EDC$. If AD, BE, and CF are concurrent and $\alpha/\beta = \delta/\gamma = m$ $(m \neq 1)$, prove that $\alpha = \delta$ and $\beta = \gamma$.

10349. *Proposed by Raphael M. Robinson, University of California, Berkeley, CA.*

The hyperbolic plane is tiled with equilateral triangles meeting seven at each vertex. Can the tiles be colored with seven colors in such a way that no two tiles of the same color meet, even at a vertex? (This problem was suggested to the proposer by David Gale.)

10350. *Proposed by Borislav Lazarov, Sofia, Bulgaria.*

Let M be a set of positive integers. Let P_M be set of all primes that divide elements of M, and let L_M be the set of elements of M having no proper divisor in M. Show that P_M finite implies L_M finite.

10351. *Proposed by Leopold Flatto and Jeffrey C. Lagarias, AT & T Bell Laboratories, Murray Hill, NJ.*

Consider the random power series

$$f(t)=\sum_{n=0}^{\infty}\eta_n t^n,$$

where the η_i are drawn independently from $\{-1, 1\}$, with the probability of $\eta_i = 1$ being p for all i.

(a) If $p = 1/2$, show that $f(t)$ has infinitely many zeros in the interval $(0, 1)$ with probability one.

(b) What happens if $p \neq 1/2$?

10352. *Proposed by Yves Nievergelt, Eastern Washington University, Cheney, WA.*

Let U be an open subset of $\mathbb{R}^n$ with smooth boundary ∂U contained in a ball of radius R.

(a) For $n = 3$, show that $\mathrm{Vol}(U) \leq R \cdot \mathrm{Area}(\partial U)/3$.

(b) Generalize to arbitrary dimensions n.

10353. *Proposed by Barry Powell, Kirkland, WA.*

Show that, for any odd prime p, there do not exist non-zero integers, x, y, z satisfying

$$(x,y)=1 \qquad p\nmid xy \quad x^6+y^6=z^p.$$

NOTES

Notes: (10347) A weaker version of this appeared as Problem A2 on the 19th Annual William Lowell Putnam Mathematical Competition (November 1958). **(10349)** Since seven triangles meet at each vertex, the angles in the triangles are all $2\pi/7$. The sum of the angles in each triangle is less than π as required in a hyperbolic plane. **(10353)** See P. Ribenboim, *Thirteen lectures on Fermat's Last Theorem*, especially pp. 67–68 where the Jacobi symbols $\left(\dfrac{Q_p}{Q_l}\right)$ are evaluated, with $Q_p = Q_p(a,b) = (b^p - a^p)/(b-a)$ with a and b odd, relatively prime, and $a \equiv b \pmod 4$. Other MONTHLY problems dealing with variations of the Fermat equation are E2771 [1979, 308; 1980, 407] and 6558 [1987, 884; 1990, 434].

SOLUTIONS

Periodicity in Multiplicative Groups

6658 [1991, 445]. *Proposed by L. Van Hamme, Free University of Brussels, Belgium.*

Define a sequence of integers by

$$a(0) = 1, \qquad a(n) = \sum_{r=0}^{n-1} \binom{n}{r} a(r) \quad \text{for } n \geq 1,$$

so that $\sum_{n=0}^{\infty} a(n)x^n/n! = (2 - e^x)^{-1}$ for $|x| < \log 2$. (This is sequence 1191 in N. J. Sloane's *Handbook of Integer Sequences*, New York, Academic Press, 1973.)

Prove that if p is a prime number and m is an integer not divisible by p, then

$$a(mp^k + s) \equiv a(mp^{k-1} + s) \pmod{p^k}$$

for k a positive integer and s a nonnegative integer.

Solution I by the proposer. Let $\mathbb{R}[X]$ be the set of all real polynomials considered as an $\mathbb{R}$-vector space and define a linear map

$$\phi\colon \mathbb{R}[X] \to \mathbb{Q} \text{ by } \phi(X^n) = a(n) \quad \text{for } n = 0, 1, 2, \ldots$$

Apply ϕ to the identity $(X+1)^n = \sum_r \binom{n}{r} X^r$. Then, for $n \geq 1$,

$$\phi((X+1)^n) = a(n) + \sum_{r=0}^{n-1} \binom{n}{r} a(r) = 2a(n) = 2\phi(X^n).$$

Hence, for any polynomial $p(X)$,

$$\phi(p(X+1)) = 2\phi(p(X)) - p(0).$$

Taking for $p(X)$ the polynomial $\binom{X}{r}$, and using the relation $\binom{X+1}{r} = \binom{X}{r} + \binom{X}{r-1}$ for all $r \geq 1$, we get

$$\phi\left(\binom{X}{r}\right) = \phi\left(\binom{X}{r-1}\right) \qquad r \geq 1.$$

Thus, ϕ sends $\binom{X}{r}$ to 1 for $r = 0, 1, 2, \ldots$. If a polynomial $p(X)$ takes only integer values for $X = 0, 1, 2, \ldots$, then $p(X)$ is of the form $p(X) = \Sigma_r c_r \binom{X}{r}$ with $c_r \in \mathbb{Z}$, and hence $\phi(p(X))$ is an integer. Now apply this observation to the polynomial

$$p(X) = \frac{X^{mp^k+s} - X^{mp^{k-1}+s}}{p^k}.$$

Since $a^{p^k} \equiv a^{p^{k-1}} \pmod{p^k}$ for all integers a, this polynomial is integer-valued; hence

$$\phi(p(X)) = \frac{a(mp^k + s) - a(mp^{k-1} + s)}{p^k}$$

is an integer, as required.

Solution II by Jens Schwaiger, Universität Graz, Graz, Austria. Since

$$\sum_{n=0}^{\infty} a(n)\frac{x^n}{n!} = (2 - e^x)^{-1} = (1 - (e^x - 1))^{-1} = \sum_{m=0}^{\infty} (e^x - 1)^m$$

and since

$$\frac{(e^x - 1)^j}{j!} = \sum_{l=0}^{\infty} S(l, j)\frac{x^l}{l!},$$

where $S(l, j)$ denotes the Stirling number of the second kind given by

$$S(l, j) = \frac{1}{j!}\sum_{i=0}^{j} (-1)^i \binom{j}{i} (j - i)^l$$

(cf. Louis Comtet, *Advanced Combinatorics*, D. Reidel, 1974, pp. 204–206) we get

$$a(n) = \sum_{j=0}^{\infty} j!S(n, j) = \sum_{j=0}^{N(n)} j!S(n, j)$$

where $N(n)$ is any integer greater than or equal to n.

Putting $n_k = mp^k + s$ and choosing $N(n_k) = N(n_{k-1}) = n_k$, we thus get

$$a(n_k) - a(n_{k-1}) = \sum_{j=0}^{n_k}\sum_{i=0}^{j} (-1)^i \binom{j}{i} (j - i)^s \left((j - i)^{mp^k} - (j - i)^{mp^{k-1}}\right)$$

yielding the desired result as in Solution I.

Editorial comment. The solutions show that the condition that $p \nmid m$ in the statement is not required.

A related use of the operator ϕ of Solution I can be found in Gian-Carlo Rota, "The number of partitions of a set," this MONTHLY, 71 (1964), 498–504.

Solved also by D. Callan, E. Dobrowolski (Canada), O. P. Lossers (The Netherlands), R. Richberg (Germany), and C. Vanden Eynden.

An Absorbing 4-Digit Number

10194 [1992, 161]. *Proposed by Jiro Fukuta, Gifu-ken, Japan.*

(a) For any four-digit number x in base 12, *excluding the eleven numbers with all digits equal*, form the number $A = a_1a_2a_3a_4$ obtained by arranging the four digits in descending order of magnitude. Next form the number $B = a_3a_4a_1a_2$ obtained by exchanging the first two with the last two digits. Put $K(x) = A - B$ and $K^{i+1}(x) = K(K^i(x))$ for $i = 1, 2, \dots$. Prove that $K^i(x) = 4378$ if $i \geq 5$.

(b) Generalize to the base $3 \cdot 2^n$, $n = 0, 1, 2, \dots$.

Solution by Robin J. Chapman, University of Exeter, United Kingdom. When giving a number by digits, we surround it by parentheses, with commas between digits if needed for clarity. Replacing 12 by $b = 3 \cdot 2^n$, we prove that $K^i(x) = (2^n, 2^n - 1, 2^{n+1} - 1, 2^{n+1})$ if $i \geq 2n + 3$ and x does not have equal digits.

We first prove $K(x)$ has the form $(\alpha, \beta, b - 1 - \alpha, b - 1 - \beta)$, with $0 \leq \alpha$, $\beta < b$. Since $(b - 1 - \alpha, b - 1 - \beta)_b = (b^2 - 1) - (\alpha\beta)_b$, the four-digit form specified equals $(b^2 - 1)[(\alpha\beta)_b + 1]$. By the definition,

$$K(x) = (b^2 - 1)\left[(a_1a_2)_b - (a_3a_4)_b\right].$$

Hence we set $(\alpha\beta)_b = (a_1a_2)_b - (a_3a_4)_b - 1$ to complete the claim. This guarantees that $K(x)$ does not have all digits equal if $n > 0$, since that requires $\alpha = b - 1 - \alpha$, but b is even. When $b = 3$, one can have $K(x) = (1111)$, but only when $A = 2210$. The 12 values of x base 3 having this A must also be excluded.

We next prove $K^2(x)$ has the form $(\gamma, \gamma - 1, b - 1 - \gamma, b - \gamma)$, with $1 \leq \gamma < b$, which we call $N(\gamma)$. By the first claim, the digits of $K(x)$ consist of two pairs summing to $b - 1$; let them be $(c_1c_2c_3c_4)$ when put in descending order. Then $K^2(x) = (\alpha', \beta', b - 1 - \alpha', b - 1 - \beta')$, where $(\alpha'\beta')_b = (c_1c_2)_b - (c_3c_4)_b - 1$. This sets $K^2(x) = N(\gamma)$ with $\gamma = c_1 - c_3$.

Now we compute $K(N(\gamma))$ for $1 \leq \gamma < b$. If $\gamma \geq (b + 1)/2$, then in descending order the digits of $N(\gamma)$ are $\gamma, \gamma - 1, b - \gamma, b - \gamma - 1$, from which we compute $K(N(\gamma)) = N(2\gamma - b)$. If $\gamma \leq (b - 1)/2$, then in descending order the digits of $N(\gamma)$ are $b - \gamma, b - \gamma - 1, \gamma, \gamma - 1$, from which we compute $K(N(\gamma)) = N(b - 2\gamma)$. Finally, if $b > 3$ we may have $\gamma = b/2$, in which case the digits of $N(\gamma)$ are $b/2, b/2, b/2 - 1, b/2 - 1$ and $K(N(\gamma)) = N(1)$. Summarizing, we have $K(N(\gamma)) = N(f(\gamma))$, where

$$f(\gamma) = \begin{cases} 1 & \text{if } \gamma = b/2 \\ |2\gamma - b| & \text{if } \gamma \neq b/2. \end{cases}$$

Note that $f(2^n) = 2^n$.

We now claim that $f^{2n+1}(\gamma) = 2^n$ for all γ with $1 \leq \gamma < b$, from which the result follows immediately. This is trivial if $b = 3$, so we may assume $n > 0$. If $\gamma \notin \{2^n, b/2, 2^{n+1}\}$, then $f(\gamma)$ is divisible by more factors of 2 than γ is. We reach $f^r(\gamma) = b/2$ for some $r \leq n - 1$ or $f^r(\gamma) \in \{2^n, 2^{n+1}\}$ for some $r \leq n$. Since $f(2^{n+1}) = f(2^n) = 2^n$, it suffices to show $f^{n+2}(b/2) = 2^n$. This follows by direct computation, since $f(b/2) = 1$ and $f^t(1) = 3 \cdot 2^n - 2^t$ for $1 \leq t \leq n + 1$.

One can give examples where $2n + 3$ iterations are needed. For $n > 0$, let $x = (b/2 + 2, b/2 + 1, 0, 0)$. Then $K^2(x) = N(3)$. Since $f^{2n}(3) = 2^{n+1}$, $K^{2n+2}(x) \neq N(2^n)$. Hence the bound $i \geq 5$ in the statement of part (a) is incorrect; $i \geq 7$ is needed.

Editorial comment. A. Tissier and S. Sagong noted that in bases other than 2 or $3 \cdot 2^n$ this iteration has no fixed point.

Solved also by J. C. Binz (Switzerland), L. Coutry (Egypt), M. Dindos (Slovakia), F. H. Kierstead, Jr., S. Sagong, R. Stong, National Security Agency Problems Group, and the proposer.

Cutting a Parameterized Circle in Half

10198 [1992, 162]. *Proposed by David M. Bloom, Brooklyn College of CUNY, Brooklyn, NY.*

Suppose f is a continuous map of $[0, 1]$ onto a circle. Prove that there exist two closed subintervals of $[0, 1]$ intersecting in at most one point whose images under f are complementary semicircles (i.e., semicircles intersecting only at their endpoints).

Solution by Richard Stong, Rice University, Houston, TX. View the circle as $\mathbb{R}/\mathbb{Z}$. Since $[0, 1]$ is simply-connected, f lifts to a continuous map $g\colon [0, 1] \to \mathbb{R}$. Let a be the maximum value that g attains and let b be a point where $g(b) = a$. Since f is onto, g must attain values arbitrarily near $a - 1$. Therefore, since g is continuous there must be some point e with $g(e) = a - 1$. Assume for definiteness that $e > b$. Let c and d be respectively the smallest and largest values in $[b, e]$ for which $g(x) = a - 1/2$. Then $[b, c]$ and $[d, e]$ are the desired intervals.

Solved also by K. F. Andersen (Canada), D. W. Bailey, W. H. Beckmann, F. Brulois, R. J. Chapman (U.K.), K. S. Kedlaya (student), Y.-H. Kiem (student, Korea), R. Martin (student), A. Müller (France), A. Nijenhuis, N. Passell, B. Richmond, A. Riese, S. T. Stefanov (Bulgaria), E. Suárez (Spain), J. Vogel, T. Zeanah & E. G. Katsoulis, Northern Kentucky University Problem Group, and the proposer. One incorrect solution was received.

Just Below the Graph of $1/(1 - x)$

10209 [1992, 266]. *Proposed by Feng Hanqiao, Shaanxi Normal University, Xian, China, and Siu-Ah Ng, University of Hull, Hull, England.*

For each non-negative integer k, define $a_k(n)$ for non-negative integers n by

$$a_k(0) = 1 \quad \text{and} \quad a_k(i + 1) = a_k(i)\left(1 + \frac{1}{k}a_k(i)\right) \quad (i \geq 0).$$

Find $\sup_n a_{mn}(n)$ for $m = 1, 2, \ldots$.

Solution by Reiner Martin (student), University of California, Los Angeles, CA. We will show that

$$\sup_n a_{mn}(n) = \begin{cases} \infty & \text{for } m = 1, \\ \dfrac{m}{m-1} & \text{for } m > 1. \end{cases}$$

These expressions follow from the inequalities

$$\frac{k}{k-n} - \frac{kn}{(k-n)^3} \leq a_k(n) \leq \frac{k}{k-n}. \tag{1}$$

The right inequality is valid when $k > n \geq 0$; the left inequality requires the

additional condition that $k \geq n + \sqrt{n}$. Given (1), set $k = mn$ to obtain the result for $m > 1$. Since $a_k(n)$ is clearly an increasing function of n for fixed k, the result for $m = 1$ will follow from the fact that the left side is unbounded as a function of n and k with $k > n$.

We prove (1) by induction on n, the case $n = 0$ being trivial. For the right side, if $k > n + 1$, the inductive step is

$$a_k(n+1) = a_k(n)\left(1 + \frac{1}{k}a_k(n)\right) \leq \frac{k}{k-n}\left(1 + \frac{1}{k}\frac{k}{k-n}\right) \leq \frac{k}{k-n-1},$$

where the rightmost inequality follows from $(k-n-1)(k-n+1) \leq (k-n)^2$. Denote the left side of (1) by $f(k,n)$. In order to use

$$f(k,n)\left(1 + \frac{f(k,n)}{k}\right) \leq a_k(n)\left(1 + \frac{a_k(n)}{k}\right) = a_k(n+1)$$

in the inductive step, we demand $f(k,n) \geq 0$, which is guaranteed by $k > n + \sqrt{n}$. This being so, we then wish to show that

$$f(k,n)\left(1 + \frac{f(k,n)}{k}\right) - f(k,n+1)$$

is positive. This is easily done using a computer algebra package. Multiplying this expression by $(k-n)^6(k-n-1)^3$ yields k times an expression which becomes

$$n^2l^3 + nl^5 + 8nl^4 + 17nl^3 + 15nl^2 + 6nl + n + 2l^5 + 9l^4 + 16l^3 + 14l^2 + 6l + 1$$

on substituting $k = n + 1 + l$. Since this is a polynomial with positive coefficients, the result follows.

Editorial comment. By various means, most solvers related $\sup_n a_{mn}$ to $\sum_{n=0}^{\infty} x^n = 1/(1-x)$. Christopher P. Grant and Thomas Kunkle did so by noting that the sequence $a_k(i)$, $0 \leq i < k$ is the approximation to the solution of $y' = y^2$, $y(0) = 1$ on $[0,1)$ generated by Euler's method with step size $1/k$.

Solved also by R. J. Chapman (U.K.), C. P. Grant, T. Kunkle, O. P. Lossers (The Netherlands), R. Stong, and the proposers.

REVIVALS

Homeomorphisms of Compact Metric Spaces

6612 [1989, 846; 1991, 663]. *Proposed by Ebrahim Salehi, University of Nevada, Las Vegas, NV.*

Suppose X is a compact metric space with metric d, and suppose $T\colon X \to X$ is continuous. If

$$\inf_{n \in \mathbb{N}} d(T^n x, T^n y) > 0$$

for each pair x, y of distinct elements of X, prove that T is onto.

Editorial comment. Shortly after the original publication of a solution, David B. Ellis, Ebrahim Salehi, and John Henry Steelman provided counterexamples to the claim, made in that solution, that

$$d'(x,y) = \inf_{n \geq 0} d(T^n x, T^n y)$$

is a metric. For example, if X consists of the three real numbers $0, 1, x$ with $0 < x < 1/2$, using the metric induced from $\mathbb{R}$, and T interchanges 0 and 1 while fixing x, then $d'(0,1) = 1 > 2x = d'(0,x) + d'(x,1)$. Deeper constructions appear to be needed to solve the problem. The following solution is based on the idea of the *enveloping semigroup*. The enveloping semigroup and related notions have proven to be extremely valuable in topological dynamics (see references). The previous argument claimed to work even when T is not assumed continuous. It is still open to decide if the assumption of continuity is required.

Solution by David B. Ellis, Beloit College, Beloit, WI. In order to define our semigroup of functions, we consider the set $X^X = \{f\colon X \to X\}$, of all self maps of X. Note that X^X is a semigroup under composition. We give X^X the topology of pointwise convergence, so that

$$f_\alpha \to f \Leftrightarrow f_\alpha(x) \to f(x) \quad \text{for every } x \in X.$$

This makes X^X a compact Hausdorff space. By analogy to the *enveloping semigroup* of (X,T), we form the closure in X^X of the strictly positive iterates of T:

$$\hat{E}(X,T) = \overline{\{T, T^2, \dots, T^n, \dots\}} \subset X^X.$$

Our solution requires two lemmas concerning $\hat{E}(X,T)$. The first lemma is an immediate consequence of the assumption that T is continuous and the fact that we have given X^X the topology of pointwise convergence.

Lemma 1. *Let X be a compact Hausdorff space and $T\colon X \to X$ be continuous. Then*

(a) *the function $L_T\colon X^X \to X^X$ defined by $L_T(p) = T \circ p$ is continuous,*
(b) *the function $R_p\colon X^X \to X^X$ defined by $R_p(q) = q \circ p$ is continuous for every $p \in X^X$,*
(c) *$\hat{E}(X,T)$ is a subsemigroup of X^X.*

Lemma 2. *Let S be a compact Hausdorff space with a semigroup structure in which R_p, defined as in Lemma* 1(b), *is continuous for every $p \in S$. Then S contains an element u with $u^2 = u$.*

Proof: We use a Zorn's lemma argument. Let

$$\mathscr{M} = \{M \subset S \mid \varnothing \neq M \text{ is closed and } M^2 \subset M\}.$$

Note that $S \in \mathscr{M}$ so $\mathscr{M}$ is nonempty. If $\{M_\alpha \mid \alpha \in A\}$ is a descending chain of elements of $\mathscr{M}$, then

$$M = \bigcap_{\alpha \in A} M_\alpha \in \mathscr{M}$$

is an infimum. Applying Zorn's lemma we get a minimal nonempty element $N \in \mathscr{M}$. Let $u \in N$. Then $R_u(N) = Nu$ is a compact, hence closed, subset of S. Since $(Nu)(Nu) = (NuN)u \subset Nu \subset N$, it follows that $Nu = N$ because N is

minimal. Now set

$$Q = \{v \in N | vu = u\} = R_u^{-1}(\{u\}) \cap N.$$

Q is nonempty because $u \in N = Nu$; Q is closed because R_u is continuous. Moreover $(v_1v_2)u = v_1(v_2u) = v_1u = u$ for any $v_1, v_2 \in Q$; thus $Q^2 = Q$. The minimality of N implies that $Q = N$. In particular $u \in Q$ so that $u^2 = u$.

We now show how the desired result follows from these two lemmas.

Since X is compact, the image of T is closed. Thus it suffices to show that the image of T is dense. To this end, choose $x \in X$ and let U be any open neighborhood of x. We will show that U intersects the image of T.

By the lemmas, we can find an idempotent $u \in \hat{E}(X,T)$. In particular

$$u(u(x)) = u(x).$$

Now u is a limit point of the strictly positive iterates of T in the topology of pointwise convergence. Thus for any neighborhood V of $u(x)$ there exists $n > 0$ such that

$$T^n(u(x)), T^n(x) \in V.$$

The assumption that $\inf d(T^n x, T^n y) > 0$ when $x \neq y$ implies that $x = u(x)$. Taking $V = U$ we have $T^n(x) \in U$, and hence U intersects the image of T.

REFERENCES

1. J. Auslander, *Minimal Flows and their Extensions*, North Holland, Amsterdam, 1988
2. D. Ellis, "What does Topological Dynamics have to do with Algebra?", *preprint*
3. R. Ellis, *Lectures on Topological Dynamics*, Benjamin, New York, 1969

Extraneous Primes

E 3452 [1991, 645]. *Proposed by C. A. Nicol and J. L. Selfridge, University of South Carolina, Columbia, SC.*

If n is an odd integer greater than 3 and ϕ is the Euler function, prove that there exists a prime p such that $p|(2^{\phi(n)} - 1)$ but $p \nmid n$.

Editorial comment. Gerry Myerson has pointed out that an extension of the result was misstated, and two values were omitted from what was claimed to be a "complete list". The items listed are the set of pairs a, n such that $(a, n) = 1$, $a > 1$ and $n > 2$ for which there is *no* prime p such that $p|(a^{\phi(n)} - 1)$ but $p \nmid n$. The complete list of such (n, a) is $\{(3,2), (4,3), (6,2), (6,3), (6,5), (6,7), (6,17), (10,3)\}$.

Source-even Orientations of Graphs

E 3462 [1991, 755; 1993, 594]. *Proposed by J. J. Rotman, University of Illinois at Urbana-Champaign, IL.*

Prove that any connected simple graph with an even number of edges has an orientation (assignment of direction to each edge) such that the number of edges leaving each vertex is even.

Editorial comment. Fred Galvin has pointed out that the word "connected" was omitted from his result for infinite graphs. A correct statement is given below.

Let G be a connected infinite graph and let V_F be the set of vertices of finite degree. Then, for any mapping $p: V_F \to \{0, 1\}$, there is an orientation of G such that, for every vertex $v \in V_F$, the number of edges leaving v has the same parity as $p(v)$.

If the graph G is allowed to have finite components, it is easy to construct counterexamples. In particular, one can take an infinite number of disjoint copies of the graph consisting of two vertices joined by a single edge, with $p(v) = 0$ for all v.

Institute For Advanced Study

In describing the new Institute for Advanced Study at Princeton, Professor Veblen said that a few years ago Mr. Bamberger decided to devote his wealth to some useful purpose and through the influence of Mr. Abraham Flexner decided to devote it to a project for the furtherance of pure scholarship. The plan contemplates a small group of mathematicians who will be free to do scientific work involving no bestowal of degrees, large liberty being allowed to the professors in conducting their activities in the form of seminars or formal lectures or none, as they may wish. It is expected that the students will be beyond the stage of the usual graduate student and that mathematicians will come to the Institute for limited periods of time for the purpose of doing some particular piece of work, for writing a book, etc.

—*American Mathematical Monthly*
40, (1933) p. 128

INDEX TO VOLUME 100, 1993
THE AMERICAN MATHEMATICAL MONTHLY

TITLE INDEX

AUTHOR INDEX

NOTES TITLE INDEX

NOTES AUTHOR INDEX

REVIEWS BY TITLE

Names of authors are in ordinary type; those of reviewers in capitals.

SOLUTIONS

Numbers in boldface refer to problems; those in lightface to pages.

PROBLEMS PROPOSED

PROBLEMS SOLVED

Thanks

The Monthly expresses its appreciation to the following people for their help in refereeing during the past year. We could not function without such people and their hard work.

David J. Aldous, Richard A. Askey, Edward J. Barbeau Jr., John Kelly Beem, Jeffrey M Bergen, Bruce Berndt, T.S. Blyth, Ken Brakke, Richard A. Brualdi, Dorothy D. Buerk, Joe Buhler, William Calhoun, Paul J. Campbell, Timothy J. Carlson, Karen L. Collins, Robert M. Corless, William H. Cunningham, Alejandro de Acosta, Robert Devaney, Edsger W. Dijkstra, Josef F. Dorfmeister, Paul Edelman, Gerald Edgar, Anthony Edwards, James F. Epperson, Clint Erb, Ron Evans, J. Douglas Faires, Lawrence A. Fialkow, Daniel Flath, Ira M. Gessel, Leonard Gilman, John Gimbel, Andrew M. Gleason, John Robert Greene, David Gries, Branko Grünbaum, William H. Gustafson, Wolfgang Haken, Philip J. Hanlon, John G. Harvey, Bruce Hill, Thomas W. Hungerford, Glenn Hurlbert, Joe Iaia, Victor Klee, Ronald Knill, Jeffrey C. Lagarias, Tsit-Yuen Lam, David J. Leeming, James MacQueen, Peter R. Massopust, Stephen B. Maurer, Albert Nijenhuis, Alec Norton, Joseph O'Rourke, Frank Okoh, Ingram Olkin, Richard Olshen, Guillermo Owen, Sharon L. Pedersen, Subramanian Ramakrishnan, Bruce Reznick, Ira Rosenholtz, Cecil C. Rousseau, Patrick J. Ryan, Marco Scarsini, Frederick Jr. Schmitt, Jeffrey Shallit, Daniel B. Shapiro, Stuart J. Sidney, Rodica Simion, Joseph H. Sliverman, Tara L. Smith, J. Laurie Snell, Hunter Snevily, G. Sparling, Joel Spencer, Ralph G. Stanton, Robert Steinberg, Lajos F. Takacs, Alan D. Taylor, Jeremy T. Teitelbaum, Alfred Jacobus Van der Poorten, David C. Vella, William Waterhouse, William Watkins, Jet Wimp, Brian J. Winkel

We give a special thanks to the Notes consultants:

John Akeroyd, Dennis Brewer, Dan Luecking, Mihalis Maliakas, Itrel Monroe, Serge Tabachnikov.